Załącznik nr 2
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

Instrukcja zarządzania systemem informatycznym

1. Wstęp.

Celem Instrukcji zarządzania system informatycznym służącym do przetwarzania danych osobowych jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu - Zdroju oraz minimalizowanie incydentów mogących zagrozić bezpieczeństwu systemu.

2. Definicje.

Ilekroć w niniejszym dokumencie jest mowa o:

a) JZK - rozumie się przez to miejską jednostkę budżetową Jastrzębski Zakładu Komunalny w Jastrzębiu - Zdroju,
b) Administratorze Danych Osobowych (ADO) - należy przez to rozumieć dyrektora JZK,
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) 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,
f) identyfikatorze użytkownika - rozumie się przez to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
g) sieci lokalnej - rozumie się przez to połączenie komputerów pracujących w JZK w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,
h) systemie informatycznym - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

3. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych w systemie informatycznym.

3.1. Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

a) ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.),
b) rozporządzeniem 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),
c) polityką bezpieczeństwa w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu - Zdroju,
d) niniejszym dokumentem.

3.2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na wykazie, którego wzór stanowi **załącznik nr 1** do niniejszego dokumentu.

3.3. Przetwarzania danych osobowych może dokonywać jedynie pracownik posiadający upoważnienie ADO. Upoważnienie zawiera określenie zbiorów danych, poziom uprawnień (administracja, edycja, wgląd), datę nadania, termin ważności i ma formę pisemną. Wzór upoważnienia stanowi **załącznik nr 2** do niniejszego dokumentu.

3.4. Upoważnienie traci ważność automatycznie w momencie ustania zatrudnienia, zmiany stanowiska pracy lub wygaśnięcia umowy.
3.5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu przez ASI dla każdego użytkownika unikalnego identyfikatora, hasła, oraz ustanowienia zakresu dostępnych danych i operacji.
3.6. Hasło pierwszego logowania w systemie informatycznym ustanawia ABI. Każdy użytkownik systemu informatycznego ma obowiązek dokonać jego zmiany na indywidualne podczas pierwszego logowania się w systemie informatycznym.
3.7. Pracownik ma prawo do wykonywania tylko tych czynności, do jakich został upoważniony.
3.8. W systemie informatycznym stosuje się uwierzytelnienie dwustopniowe: na poziomie dostępu do sieci lokalnej, oraz dostępu do aplikacji.
3.9. Odebrania uprawnień pracownikowi dokonuje Administrator Danych Osobowych z podaniem daty i przyczyny odebrania uprawnień.
3.10. Kierownicy komórek organizacyjnych zobowiązani są informować Administratora Danych Osobowych o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
3.11. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, oraz unieważnić jej hasło.

4. Zasady ustalania i posługiwania się hasłami.

4.1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
4.2. Hasło użytkownika musi być zmienione przynajmniej jeden raz w miesiącu.
4.3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźniej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4.4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
4.5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
4.6. Pracownik nie ma prawa udostępniania swojego hasła innym osobom.
4.7. Hasło należy wprowadzać w sposób, który uniemożliwi innym osobom jego poznanie.
4.8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
4.9. Minimalna długość hasła nie może mieć mniej niż 8 znaków i winno zawierać równoczesną kombinację liter, cyfr i znaków specjalnych.
4.10. Przy wyborze hasła zakazuje się stosować:
   a) haseł, z których użytkownik korzystał w poprzednim miesiącu,
   b) swojej nazwy użytkownika w jakiejkolwiek formie,
   c) swojego nazwiska czy imienia w jakiejkolwiek formie,
   d) ogólnie dostępnych informacji o użytkowniku takich jak numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka itp.
   e) przewidywalnych sekwencji znaków z klawiatury np. „QWERTY”,”12345” itp.
4.11. Zmiany hasła nie można zlecać innym użytkownikom.

5. Rejestr użytkowników upoważnionych do przetwarzania danych osobowych.

5.1. ABI jest zobowiązany do prowadzenia rejestru użytkowników upoważnionych do przetwarzania danych osobowych oraz i ich uprawnień w systemie informatycznym.
5.2. Rejestr musi odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwić przeglądanie historii zmian w systemie informatycznym.

5.3. Wzór rejestru użytkowników upoważnionych do przetwarzania danych osobowych stanowi **załącznik nr 3** do niniejszego dokumentu.

6. Procedury rozpoczęcia, zawieszania i zakończenia pracy w systemie.

6.1. Przed rozpoczęciem pracy z komputerem należy zalogować się do systemu informatycznego przy użyciu własnego indywidualnego identyfikatora i hasła.
6.2. W sytuacji opuszczenia stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu.
6.3. Przed wyłączeniem komputera należy zakończyć pracę wszystkich używanych programów i wykonać o ile to możliwe prawidłowe zamknięcie systemu.
6.4. Niedopuszczalne jest wyłączanie komputera bez prawidłowego zamknięcia wszystkich programów i wylogowania z sieci komputerowej.
6.5. Przypadki nieprawidłowej pracy systemu informatycznego należy niezwłocznie zgłaszać ASI.

7. Kopie bezpieczeństwa danych osobowych.

7.1. Kopie bezpieczeństwa danych osobowych wykonywane są przez ASI.
7.2. Kopie bezpieczeństwa wykonywać należy po każdym dniu roboczym na zewnętrznych dyskach HDD.
7.3. Dyski zewnętrzne HDD z kopiami bezpieczeństwa po archiwizacji przechowywane są w szafie stalowej w zamkniętym pomieszczeniu.

8. Postępowanie z elektronicznymi nośnikami informacji zawierających dane osobowe oraz wydrukami.

8.1. Wymienne elektroniczne nośniki informacji należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych,
8.2. Do zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji należy przechowywać wyłącznie w zamykanych szafach biurowych,
8.3. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych,
8.4. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych. W przypadku, gdy nie jest to możliwe uszkadza się je w sposób uniemożliwiający ich odczytanie,
8.5. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
8.6. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym dostęp osobom nieuprawnionym,
8.7. Pomieszczenie, w którym przechowywane są wydruki musi być zamknięte na klucz po godzinach pracy JZK,
8.8. Wydruki zawierające dane osobowe w momencie przekazania do usunięcia są niszczone w sposób uniemożliwiający ich odczytanie (w specjalnej niszczarce do papieru).

9. Ochrona przed złośliwym oprogramowaniem.

9.1. Każdy komputer służący do przetwarzania danych osobowych winien być wyposażony w działający cały czas program antywirusowy. Program antywirusowy winien aktualizować się na bieżąco w sposób automatyczny.

9.2. Zabrania się stosowania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Za skanowanie odpowiedzialny jest użytkownik komputera.
9.3. Poczta elektroniczna winna być sprawdzana automatycznie przez skaner antywirusowy.
9.4. Wykrycie wirusa użytkownik komputera ma obowiązek zgłosić natychmiast Administratorowi Systemu Informatycznego.
9.5. ASI przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach systemu nie rzadziej niż raz w miesiącu. Z kontroli tych sporządza się protokół zgodnie z **załącznikiem nr 4** do niniejszego dokumentu.

10. Połączenie do sieci Internet.

10.1. Połączenie z siecią Internet zabezpieczony winien być przez moduł firewall działający na routerze sieciowym.
10.2. Na każdym komputerze w systemie informatycznym JZK winien działać osobny firewall.
10.3. Zabronione jest łączenie się z siecią Internet poprzez komputer z niedziałającym lub wyłączonym programem antywirusowym i firewallem.

11. Procedura postępowania w sytuacji naruszenia polityki bezpieczeństwa.

11.1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym ABI lub inną upoważnioną osobę.
11.2. ABI (lub upoważniona osoba) w porozumieniu z ASI po otrzymaniu powiadomienia:
a) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
b) sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
c) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
d) sprawdza zawartość zbioru danych osobowych,
e) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.
11.3. W przypadku stwierdzenia naruszenia zabezpieczeń danych ASI:
a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),
b) w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła konta administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
c) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
d) niezwłocznie przywraca prawidłowy stan działania systemu,
e) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
f) sporządza raport z naruszenia bezpieczeństwa danych osobowych, którego wzór stanowi **załącznik nr 5** do niniejszego dokumentu.
11.4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) ASI przekazuje ABI.
11.5. ASI w porozumieniu z ABI, podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
a) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu,uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń

i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

b) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągnięcie konsekwencji przewidzianych prawem,

c) jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organy ścigania.

12. Spis załączników.

Załącznik nr 1 - Wzór oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych w Jastrzębskim Zakładzie Komunalnym.
Załącznik nr 2 - Wzór upoważnienia o przetwarzaniu danych osobowych.
Załącznik nr 3 - Wzór rejestru użytkowników systemu informatycznego upoważnionych do przetwarzania danych osobowych.
Załącznik nr 4 - Wzór protokołu z kontroli antywirusowej systemu informatycznego.
Załącznik nr 5 - Wzór raportu z naruszenia bezpieczeństwa danych osobowych.

Załącznik Nr 1
do Instrukcji zarządzania systemem informatycznym
w Jastrzębskim Zakładzie Komunalnym
w Jastrzębiu - Zdroju.

WZÓR

OŚWIADCZENIE

Niniejszym oświadczam, iż zapoznałem się przepisami zawartymi w:

a) ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.),
b) rozporządzeniu 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),
c) polityce bezpieczeństwa w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu - Zdroju,
d) instrukcji zarządzania systemem informatycznym w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu-Zdroju,

i zobowiązuje się do ich przestrzegania. Jednocześnie zobowiązuję się do zachowania w tajemnicy, także po ustaniu stosunku zatrudnienia, przetwarzanych przeze mnie danych osobowych, a także sposobów ich ochrony.

Lp.	Imię, nazwisko	Data	Podpis
1			
2			
3			
4			

Załącznik Nr 2
do Instrukcji zarządzania systemem informatycznym
w Jastrzębskim Zakładzie Komunalnym
w Jastrzębiu - Zdroju.

WZÓR

Jastrzębie - Zdrój, dnia .....

UPOWAŻNIENIE

do przetwarzania danych osobowych

Nr .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) z dniem ..... upoważniam Panią / Pana:

....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu-Zdroju

na stanowisku: .....

do przetwarzania danych osobowych w zbiorze: .....

.....

.....

z uprawnieniami: administracji / edycji / wglądu*.

Nadaję Pani / Panu identyfikator: .....

Upoważnienie ważne jest do dnia: .....

.....

(podpis administratora danych osobowych)

.....

(podpis pracownika)

Załącznik Nr 3
do Instrukcji zarządzania systemem informatycznym
w Jastrzębskim Zakładzie Komunalnym
w Jastrzębiu - Zdroju.

WZÓR

REJESTR

użytkowników systemu informatycznego

upoważnionych do przetwarzania danych osobowych

L.p.	Imię, nazwisko	Identyfikator użytkownika	Zakres uprawnienia *)	Data nadania uprawnień	Data odebrania, wygaśnięcia uprawnień	Przyczyna odebrania, wygaśnięcia uprawnień	Podpis administratora bezpieczeństwa informacji
1							
2							
3							
4							

*) Zakres uprawnień: A - administracja, E- edycja, W - wgląd

Załącznik Nr 4
do Instrukcji zarządzania systemem informatycznym
w Jastrzębskim Zakładzie Komunalnym
w Jastrzębiu - Zdroju.

WZÓR

PROTOKÓŁ

z przeprowadzenia kontroli antywirusowej systemu informatycznego Jastrzębskiego Zakładu Komunalnego w Jastrzębiu-Zdroju.

L.p.	Data kontroli	Wynik kontroli			Podpis administratora systemu informatycznego
		System czysty	Wykryto zagrożenie		
1			Lokalizacja komputera		
			Rodzaj zagrożenia		
			Podjęte czynności		
2			Lokalizacja komputera		
			Rodzaj zagrożenia		
			Podjęte czynności		
3			Lokalizacja komputera		
			Rodzaj zagrożenia		
			Podjęte czynności		
4			Lokalizacja komputera		
			Rodzaj zagrożenia		
			Podjęte czynności		

Załącznik Nr 5
do Instrukcji zarządzania systemem informatycznym
w Jastrzębskim Zakładzie Komunalnym
w Jastrzębiu - Zdroju.

WZÓR

RAPORT
z naruszenia bezpieczeństwa danych osobowych w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu - Zdroju

1. Data: ....., Godzina: .....

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. Przyczyny wystąpienia zdarzenia:
.....
.....
.....

6. Podjęte działania:
.....
.....
.....

7. Postępowanie wyjaśniające:
.....
.....
.....

.....
(data, podpis administratora systemu informatycznego)