Uchwała Nr 17/IV/2016

Zarządu Międzygminnego Związku Komunikacyjnego w Jastrzębiu-Zdroju

z dnia 26 kwietnia 2016 roku

w sprawie: przyjęcia instrukcji „Polityka Bezpieczeństwa" oraz ustalenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze zbiorów Międzygminnego Związku Komunikacyjnego z siedzibą w Jastrzębiu-Zdroju

Na podstawie art. 7 ust 1 pkt 2, art.7 ust.4, art. 8 pkt 2 oraz art.15 ust.1 pkt 10 ustawy o publicznym transporcie zbiorowym (Dz.U. z 2011 roku, Nr 5 poz.13), art. 73 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jednolity z 2013 roku, Dz. U. poz. 594 z późn. zm.) oraz § 18 pkt 1 Statutu Międzygminnego Związku Komunikacyjnego w Jastrzębiu-Zdroju

Zarząd Związku u c h w a l a :

§ 1

1. Przyjąć instrukcję „Polityka Bezpieczeństwa" w Międzygminnym Związku Komunikacyjnym z siedziba w Jastrzębiu-Zdroju wraz z załącznikami a stanowiącą Załącznik nr 1 do niniejszej uchwały.
2. Przyjąć „Instrukcję Zarządzania Systemem Informatycznym" wraz z załącznikami a stanowiącą Załącznik nr 2 do niniejszej uchwały.
3. Powierzyć prawa i obowiązki Administratora Danych Osobowych Dyrektorowi Biura Związku.

§ 2

Wykonanie uchwały powierza się Przewodniczącemu Zarządu.

§ 3

Traci moc uchwała nr 36/X/2011 z dnia 05 października 2011 roku.

§ 4

Uchwała wchodzi w życie z dniem podjęcia.

RADCA PRAWNY
Andrzej Kozar

PRZEWODNICZĄCY ZARZĄDU MZK
mgr Daniel Wawrzyczek

Załącznik nr 1
do uchwały Zarządu nr 17/IV/2016
z dnia 26.04.2016 r.

POLITYKA BEZPIECZEŃSTWA

Zgodnie z **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. Nr 100, poz. 1024)
wdraża dokument o nazwie „Polityka Bezpieczeństwa". Zapisy tego dokumentu wchodzą w życie

z dniem 26.04.2016

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzębiu-Zdroju , określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
7. administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8. podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Upoważnienie dla **Administratora Bezpieczeństwa Informacji** oraz zakres obowiązków określa **załącznik do „Polityki Bezpieczeństwa" nr 1.**

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa" nr 2.**

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik do „Polityki Bezpieczeństwa" nr 3.**

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik do „Polityki Bezpieczeństwa" nr 4.**

§ 7.

W podmiocie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych**. **Administrator Danych** stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Danych nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie upoważnienia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**. Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6** do „Polityki Bezpieczeństwa".
2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – **załącznik nr 7** do „Polityki Bezpieczeństwa".
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych - **załącznik nr 8** do „Polityki Bezpieczeństwa".

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **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**

§ 13.

Deklaracja intencji, cele i zakres polityki bezpieczeństwa

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.

2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.

3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

5. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
   b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.

8. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
   b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;

c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
d) monitorowanie zastosowanych środków ochrony;
e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.

9. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów ustawy oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

PRZEWODNICZĄCY ZARZĄDU MZK
mgr Daniel Wawrzyczek

RADCA PRAWNY
Andrzej Kocur

Jastrzębie Zdrój.....
miejscowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 2. Polityki Bezpieczeństwa z dnia 26.04.2016 zgodnie z założeniami
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

Na podstawie art. 36a ust. 1 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014 r. poz. 1182, 1662)

Administrator Danych ..... – Dyrektor Biura MZK powołuje w podmiocie Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzębiu-Zdroju NIP: 633-14-01-664

Administratora Bezpieczeństwa Informacji *(imię i nazwisko)* .....

Upoważnienie jest ważne od chwili podpisania przez strony do dnia odwołania Administratora Bezpieczeństwa Informacji przez Administratora Danych Osobowych.

Zgodnie z art. 36a ust.2 **do zadań ABI należy:**

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych,
2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji nadzoruje opracowanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych. Jest odpowiedzialny za przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. **Administrator Bezpieczeństwa Informacji** prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie, a w szczególności:

zgodnie z § 4. „Polityki Bezpieczeństwa"

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który określa załącznik do „Polityki Bezpieczeństwa" nr 2,

zgodnie z § 5. „Polityki Bezpieczeństwa"

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych

do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa" nr 3,

zgodnie z § 6. „Polityki Bezpieczeństwa"

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa" nr 4,

zgodnie z § 8. „Polityki Bezpieczeństwa"

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa" oraz zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – załącznik nr 7 do „Polityki Bezpieczeństwa".

Administrator Bezpieczeństwa Informacji sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla administratora danych lub na wniosek GIODO zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator danych zapewnia środki i organizacyjną odrębność Administratora Bezpieczeństwa Informacji niezbędne do należytego wykonywania przez niego zadań wynikających z niniejszego upoważnienia i przepisów ustawy.

OŚWIADCZENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako administrator bezpieczeństwa informacji, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzębiu-Zdroju zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Oświadczam, że spełniam wymogi dotyczące osoby powołanej na stanowisko Administratora Bezpieczeństwa informacji tj.:

- nie byłam/byłem karana/y za umyślne przestępstwo,
- posiadam pełną zdolność do czynności prawnych oraz korzystam z pełni praw publicznych,
- posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji

.....

Podpis

Administrator Danych Osobowych

.....

Podpis

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

załącznik do „Polityki Bezpieczeństwa" nr 2 zgodnie z § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	Dokładny adres *(np. adres siedziby firmy gdzie przetwarzane są dane)*	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1		Serwerownia	Podwójne drzwi obite blachą, zamykane na dwa zamki, monitoring drzwi wejściowych, pomieszczenie bez okien	
2.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1	Dział Finansowo-Księgowy, Referat Księgowo-Budżetowy	8	Drzwi zamykane na klucz	
3.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1	Dział Finansowo-Księgowy, Główna Księgowa	5	Drzwi zamykane na klucz	
4.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1	Dział Finansowo-Księgowy, Referat Biura Obsługi Klienta	1	Drzwi zamykane na klucz, monitoring pomieszczenia	
5.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1	Dział Kontroli i Nadzoru Ruchu	2,3	Drzwi zamykane na klucz	
6.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1	Dyrektor Biura	5	Drzwi zamykane na klucz	
7.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1	Dział Planowania i Organizacji Komunikacji	9	Drzwi zamykane na klucz, monitoring drzwi wejściowych	

Lp.	Dokładny adres *(np. adres siedziby firmy gdzie przetwarzane są dane)*	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
8.	44-335 Jastrzębie Zdrój ul. Przemysłowa 1	Stanowisko Administracyjne	5	Drzwi zamykane na klucz, monitoring rejonu drzwi wejściowych	

Data i podpis Administratora Danych

.....

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

załącznik do „Polityki Bezpieczeństwa" nr 3 zgodnie, z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Uwagi**
1.	Zbiór danych dłużników	Wersja papierowa i elektroniczna – INDYKATOR oraz MICROSOFT OFFICE	
2.	Zbiór danych pasażerów kupujących bilety imienne	Wersja papierowa i elektroniczna - MUNICOM	
3.	Zbiór danych kancelarii MZK - korespondencja	Wersja papierowa i elektroniczna – MICROSOFT OFFICE	

Data i podpis Administratora Danych

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami - załącznik do „Polityki Bezpieczeństwa" nr 4 zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Struktura zbiorów** *(np. imię i nazwisko, e-mail, telefon itd.)*	**Przepływ danych** (np. wydruk danych z internetu)	**Uwagi**
1.	Zbiór danych dłużników	Imię i nazwisko. PESEL. Imię ojca i matki. Data i miejsce urodzenia. Seria i numer dokumentu tożsamości. Adres zamieszkania. Miejsce , data i godzina sporządzenia protokołu kontroli. Sygnatury postępowania sądowego i odwoławczego.	Wersja papierowa -> program Windykator -> wydruki	
2.	Zbiór danych pasażerów kupujących bilety imienne	Imię i nazwisko. PESEL. Adres zamieszkania. Adres poczty elektronicznej Podstawa ulgi. Zdjęcie.	Wersja papierowa i elektroniczna -> program MUNICOM -> wydruki	
3.	Zbiór danych kancelarii MZK - korespondencja	Korespondencja kancelaryjna	Wersja papierowa -> elektroniczna oraz wersja elektroniczna -> wersja papierowa	

Data i podpis Administratora Danych

.....

Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa" zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

..... – Dyrektor Biura MZK jako Administrator Danych

dnia ..... nadaje upoważnienie do przetwarzania danych osobowych w podmiocie Międzygminny Związek Komunikacyjny z siedzibą w Jastrzębiu-Zdroju dla:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

.....

.....

.....

Upoważnienie nadaje się do dnia: na czas pełnienia obowiązków służbowych.

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182,1662) oraz 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Administrator Danych

.....

Podpis

Użytkownik

.....

Podpis

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie

załącznik nr 6 do „Polityki Bezpieczeństwa" zgodnie z Art 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*

Data i podpis Administratora Danych

.....

Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

załącznik nr 7 do „Polityki Bezpieczeństwa" zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Lp.	Rodzaj udostępnionych danych osobowych	Data wprowadzenia danych do zbioru	Data przekazania danych osobowych	Imię i nazwisko osoby która otrzymała dane	Cel przekazania danych osobowych

Data i podpis Administratora Danych

.....

Załącznik nr 2
do uchwały Zarządu nr 17/IV/2016
z dnia 26.04.2016 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Zgodnie z **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
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją".
Zapisy tego dokumentu wchodzą w życie z dniem 26.04.2016

Ilekroć w „instrukcji" jest mowa o:

1) podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
7) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w podmiocie Międzygminny Związek Komunikacyjny z siedzibą w Jastrzębiu Zdroju zapisów „instrukcji" odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji**

§2

W związku z tym, że w podmiocie Międzygminnym Związku Komunikacyjnym z siedzibą w Jastrzębiu Zdroju przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

- poprzez zainstalowanie programu antywirusowego o nazwie ESET Endpoint Security
- poprzez zainstalowanie firewall (zapora sieciowa).
- poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym Serwerownia oraz pokój nr 1 zaopatrzonym w system alarmowy.

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu.
W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§6

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7.

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **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**

PRZEWODNICZĄCY ZARZĄDU MZK
mgr Daniel Wawrzyczek

RADCA PRAWNY
Andrzej Kozar