ZARZĄDZENIE NR 35 /2015
Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu
z dnia 23.06. 2015 r.

w sprawie wprowadzenia Polityki bezpieczeństwa informacji i Instrukcji zarządzania systemem informatycznym w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu..

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014r., poz. 1182 z późn. zm.), § 3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz.1024) oraz § 13 ust. 3 pkt 1 oraz § 34 ust. 1 pkt 2 Regulaminu organizacyjnego Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu wprowadzonego Zarządzeniem Nr 57/2014 Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia 02.07.2014r. z późn. zm. sprawie wprowadzenia Regulaminu Organizacyjnego Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu, zarządzam co następuje:

§ 1

1. Wprowadzam do stosowania w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu Politykę bezpieczeństwa informacji stanowiącą załącznik Nr 1 do zarządzenia oraz Instrukcję zarządzania systemem informatycznym stanowiącą załącznik Nr 2 do zarządzenia.

§ 2

1. Wykonanie zarządzenia powierza się Administratorowi bezpieczeństwa informacji.

§ 3

1. Traci moc Zarządzenie Nr 51/2007 Dyrektora Zarządu Dróg i Komunikacji w Wałbrzychu z dnia 06.07.2007r. w sprawie wprowadzenia:
   1. polityki bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym i tradycyjnym,
   2. instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych,
   3. instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczona dla osób zatrudnionych w Zarządzie Dróg i Komunikacji w Wałbrzychu przy przetwarzaniu tych danych.

§ 4

1. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Krzysztof Szaweczyk

Załącznik Nr 1do Zarządzenia Nr 35 /2015
Dyrektora Zarządu Dróg, Komunikacji i Utrzymania
Miasta w Wałbrzychu z dnia 23.06.2015 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZARZĄDZIE DRÓG, KOMUNIKACJI I UTRZYMANIA MIASTA W WAŁBRZYCHU

I. POSTANOWIENIA OGÓLNE

§ 1.

1. Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa informacji, w tym danych osobowych, zawartych w systemach informatycznych i tradycyjnych w Zarządzie Dróg Komunikacji i Utrzymania Miasta w Wałbrzychu.
2. Celem Polityki Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących przepisów prawa w zakresie ochrony danych osobowych, sposobu przetwarzania w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu informacji zawierających dane osobowe.
3. Politykę Bezpieczeństwa opracowano na podstawie:
   1) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz.1182 z późn. zm.),
   2) 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).
   3) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r. Poz. 526).

§ 2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:
1. ZDKiUM – Zarząd Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu,
2. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. przetwarzanie danych osobowych – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. użytkownik – osoba upoważniona do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym,
5. administrator systemu informatycznego – osoba upoważniona do zarządzania systemem informatycznym – zewnętrzna firma informatyczna posiadająca upoważnienie administratora danych do administrowania zasobami danych ZDKiUM oraz nadzoru nad poprawnością stosowanych procedur zabezpieczenia danych,
6. administrator bezpieczeństwa informacji – osoba upoważniona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych,
7. system informatyczny – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,
8. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§ 3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez ZDKiUM informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki Bezpieczeństwa.
2. Wyżej wymienione pojęcia w odniesieniu do informacji i aplikacji oznaczają:
   1) Poufność informacji – zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) Zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3. Zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
   3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

§ 4.

1. W systemie informacyjnym ZDKiUM przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Informacje te są przetwarzane i składowane zarówno w postaci tradycyjnej jak i elektronicznej.

§ 5.

1. Politykę Bezpieczeństwa stosuje się do:
   1) danych osobowych przetwarzanych w systemie informatycznym,
   2) wszystkich informacji dotyczących danych pracowników ZDKiUM, w tym danych osobowych personelu oraz treści zawieranych umów o pracę,
   3) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
   4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
   5) rejestru osób dopuszczonych do przetwarzania danych osobowych,
   6) innych dokumentów zawierających dane osobowe.

§ 6.

1. Zakres określony przez dokumenty Polityki Bezpieczeństwa ma zastosowanie do całego systemu informacyjnego ZDKiUM w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz tradycyjnych, w których przetwarzane są informacje podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   3) wszystkich pracowników w rozumieniu przepisów Kodeksu pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 7.

1. Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§ 8.

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Dokumenty Polityki Bezpieczeństwa składają się z:
   1) Niniejszej Polityki Bezpieczeństwa,
   2) Instrukcji zarządzania systemami informatycznym. Określa ona sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych przez administratora danych w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem. Opisuje nadawanie uprawnień użytkownikom, określa sposoby pracy w systemie informatycznym oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego w ZDKiUM.

V. DOSTĘP DO INFORMACJI

§ 9.

1. Wszystkie osoby, których rodzaj wykonywanej pracy wiąże się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w ZDKiUM zasad ochrony danych osobowych.
2. Osobę dopuszczoną do przetwarzania danych osobowych powinna posiadać upoważnienie do ich przetwarzania (wzór upoważnienia stanowi załącznik nr 1). Osobę taką wskazuje administratorowi bezpieczeństwa informacji kierownik, bezpośredni przełożony lub osoba zatrudniona na samodzielnym stanowisku.

§ 10.

1. Dane osobowe podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, mogą być udostępnione jeżeli podmioty te w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

§ 11.

1. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§ 12.

1. Administratorem danych osobowych jest dyrektor Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu.

§ 13.

1. Za bezpieczeństwo danych osobowych ZDKiUM, odpowiadają:
   1) Administrator danych osobowych – dyrektor,
   2) Administrator bezpieczeństwa informacji – wyznaczany przez administratora danych zgodnie z art. 36 a ustawy, nadzorujący przestrzeganie zasad ochrony przetwarzania danych osobowych.
   3) Administrator systemu informatycznego – zewnętrzna firma informatyczna w zakresie objętym umową .
2. Administrator bezpieczeństwa informacji realizując politykę bezpieczeństwa informacji ma prawo wydawać instrukcje regulujące kwestie związane z ochroną danych w strukturze ZDKiUM.
3. W umowach zawieranych przez ZDKiUM powinny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez ZDKiUM.

§ 14.

1. Zapoznanie się z dokumentami określonymi w § 8 pkt 2 pracownicy ZDKiUM zatrudnieni przy przetwarzaniu danych osobowych potwierdzają podpisaniem oświadczenia (wzór oświadczenia stanowi załącznik Nr 2), które przekazują Administratorowi bezpieczeństwa informacji.

§ 15.

1. Ochrona zasobów danych osobowych jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników ZDKiUM.

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§ 16.

1. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik ZDKiUM.

§ 17.

1. Administrator bezpieczeństwa informacji w ZDKiUM:
   1) odpowiada za realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora bezpieczeństwa informacji,
   2) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
   3) określa strategię zabezpieczania systemów informatycznych ZDKiUM,
   4) sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   5) sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których przetwarzane są dane osobowe,
   6) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych ZDKiUM, zgodnie z zasadami analizy ryzyka określonymi w procedurach kontroli zarządczej w ZDKiUM.
   7) określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
   8) sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, w których przetwarzane są dane osobowe,
   9) sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
   10) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
   11) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
   12) zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
   13) powiadamia administratora systemu o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
   14) prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
   15) prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych,
   16) prowadzi ewidencję miejsc przetwarzania danych osobowych, poprzez określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego (wzór ewidencji stanowi załącznik Nr 3),
   17) prowadzi wykaz (rejestr) zbiorów danych osobowych ZDKiUM przetwarzanych metodą tradycyjną lub w systemach informatycznych z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy o ochronie danych osobowych, zawierający nazwę zbioru oraz następujące informacje;

   a) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania,
   b) oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art.31 a ustawy ochronie danych osobowych, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi,
   c) podstawę prawną upoważniającą do prowadzenia zbioru danych,

d) cel przetwarzania danych,
e) opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,
f) sposób zbierania oraz udostępniania danych, w szczególności informację, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnionym na podstawie przepisów prawa.
g) informacje o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane.

18) sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla administratora danych osobowych, Sprawozdanie powinno zawierać:
a) oznaczenie administratora, danych i adres jego siedziby lub miejsca zamieszkania,
b) imię i nazwisko administratora bezpieczeństwa informacji,
c) wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach,
d) datę rozpoczęcia i zakończenia sprawdzenia,opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
e) stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracający stan zgodny z prawem,
f) wyszczególnienie załączników stanowiących składową cześć sprawozdania,
g) podpis administratora bezpieczeństwa informacji a w przypadku sprawozdania w postaci papierowej - dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania,
h) datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.

19)nadzoruje opracowywanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2 ustawy, oraz przestrzeganie zasad w niej określonych,

20) zapewnia zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

§ 18.

1. Administrator Systemu Informatycznego odpowiedzialny jest za:
   1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   2) optymalizację wydajności systemu informatycznego, baz danych,
   3) instalację i konfigurację sprzętu sieciowego i serwerowego,
   4) instalację i konfigurację oprogramowania systemowego, sieciowego, oprogramowania baz danych,
   5) konfigurację i administrację oprogramowaniem systemowym sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
   7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,
   8) zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   10) przyznawanie na wniosek Administratora danych ściśle określonych praw dostępu do informacji w danym systemie,
   11) wnioskowanie do Administratora danych w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
   12) zarządzanie licencjami i procedurami ich dotyczącymi,

13) prowadzenie profilaktyki antywirusowej.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§ 19.

1. Przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby, w wyznaczonych pomieszczeniach zamykanych na klucz.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 20.

1. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem administratora systemu informatycznego.

IX. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 21.

1. W ZDKiUM rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:
   1) Zabezpieczenia fizyczne:
      a) pomieszczenia zamykane na klucz,
      b) szafy z zamkami,
   2) Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
      a) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
      b) przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
   3) Zabezpieczenia organizacyjne:
      a) osobą odpowiedzialną za bezpieczeństwo danych jest Administrator bezpieczeństwa informacji,
      b) Administrator bezpieczeństwa informacji na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,
   4) Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
      a) wykaz pracowników ZDKiUM uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora bezpieczeństwa informacji,
      b) przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora danych osobowych ,
      c) w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
      d) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych

osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,

e) w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego nieupoważnione,

f) po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

5) Wszystkie stanowiska komputerowe wyposażone są w indywidualna ochronę antywirusową,

6) Osoba postronna nie ma możliwości użytkowania komputera, na którym znajdują się lub są przetwarzane dane osobowe, ponieważ każdy komputer zabezpieczony jest przez indywidualny identyfikator użytkownika i cyklicznie zmieniane hasło.

X. OPIS STYRUKTURY ZBIORÓW DANYCH

§ 22

1. W ZDKiUM prowadzi się opis struktury zbiorów danych wskazujący zwartość poszczególnych pól informacyjnych i powiązania między nimi. (wzór opisu stanowi załącznik załącznik nr 4)
2. Administrator bezpieczeństwa informacji prowadzi nadzór nad aktualnością opisu struktury.

XI SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI

§ 23.

1. Przepływ danych pomiędzy systemami informatycznymi następuje w sposób manualny.

XII. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§24.

1. Archiwizacja informacji zawierających dane osobowe odbywa w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonych pomieszczeniach, które są zabezpieczone przed dostępem osób nieupoważnionych.

2. Dane w wersji papierowej są archiwizowane zgodnie z obowiązującą instrukcją archiwizacyjną.

23.06.2015r
(data i podpis dyrektora ZDKiUM)

DYREKTOR
Krzysztof Szewczyk

Załącznik Nr 1 do Polityki Bezpieczeństwa Informacji
w Zarządzie Dróg, Komunikacji i Utrzymania Miasta
w Wałbrzychu

Wałbrzych, dnia .....

Upoważnienie imienne
do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz.1182 z późn. zm.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w

.....

(nazwa jednostki i komórki organizacyjnej)

na stanowisku: .....

do przetwarzania od dnia ..... r. danych osobowych w zakresie:

.....

i nadaję identyfikator: .....

.....

Załącznik Nr 2
do Polityki Bezpieczeństwa Informacji
w Zarządzie Dróg, Komunikacji i Utrzymania Miasta
w Wałbrzychu

Wałbrzych, dnia .....

.....
(imię oraz nazwisko pracownika)

.....
(dział oraz zajmowane stanowisko)

OŚWIADCZENIE

Oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz.1182 z późn. zm.) oraz rozporządzeniami wykonawczymi wydanymi na jej podstawie.
Zapoznałam/em się i zobowiązuję się do stosowania i przestrzegania zasad dotyczących ochrony danych osobowych opisane w:

1) Polityce Bezpieczeństwa Informacji w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu,
2) Instrukcji zarządzania systemami informatycznym w Zarządzie Dróg Komunikacji i Utrzymania Miasta w Wałbrzychu.

.....
(podpis pracownika)

Załącznik Nr 3
do Polityki Bezpieczeństwa Informacji
w Zarządzie Dróg, Komunikacji i Utrzymania Miasta
w Wałbrzychu

WYKAZ POMIESZCZEŃ (OBSZARÓW), W KTÓRYCH SĄ PRZETWARZANE, PRZECHOWYWANE ORAZ NISZCZONE DANE OSOBOWE:

Zarząd Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu zajmuje pomieszczenia zlokalizowane w budynku przy ul. Jana Matejki 1:

1. **Główny Specjalista ds. Inwestycji i Remontów** zajmuje pomieszczenie/a nr 20 na I piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

2. **Dział Drogowy** zajmuje pomieszczenie/a nr 23,24,25,26,27,29 na II piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

3. **Dział Organizacji, Zarządzania i Kadr** zajmuje pomieszczenie/a nr 5,5a na parterze i 37 na I piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

4. **Zespół ds. Przetargów i Umów** zajmuje pomieszczenie/a nr 20 na I piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

5. **Zespół Radców Prawnych** zajmuje pomieszczenie/a nr 35 na II piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

6. **Główny Specjalista ds. Kontroli** zajmuje pomieszczenie/a nr 35 na II piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

7. **Główny Specjalista ds. BHP i P.poż** zajmuje pomieszczenie/a nr 35 na II piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

8. **Dział Komunikacji Zbiorowej** zajmuje pomieszczenie/a nr 6, 6a,6b na parterze oraz 17 i 18 na I piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja

zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach oraz szafach pancernych.

W punktach Sprzedaży Biletów na Placu Grunwaldzkim i Piaskowej Górze Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach oraz szafach pancernych.

9. **Dział Utrzymania Miasta** zajmuje pomieszczenie/a nr 39,40 na II piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w zamykanych na klucz szafach.

10. **Dział Finansowo-Księgowy** zajmuje pomieszczenie/a nr 30,31,32,33,34 na II piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest w szafach drewnianych zamykanych na klucz..

Załącznik Nr 4
do Polityki Bezpieczeństwa Informacji
w Zarządzie Dróg, Komunikacji i Utrzymania Miasta
w Wałbrzychu

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJACY ZAWRTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNMYCH I POWIĄZAŃ POMIĘDZY NIMI

1. Miejsce funkcjonowania programu : .....

1.1. Nazwa programu : .....
1.2. Pola danych

Załącznik Nr 2 do Zarządzenia Nr 35 /2015
Dyrektora Zarządu Dróg, Komunikacji i Utrzymania
Miasta w Wałbrzychu z dnia 23.06.2015r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W ZARZĄDZIE DRÓG, KOMUNIKACJI I UTRZYMANIA MIASTA W WAŁBRZYCHU

I. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym również do przetwarzania danych osobowych przez administratora danych w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem. Opisuje nadawanie uprawnień użytkownikom, określa sposoby pracy w systemie informatycznym oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu.
Instrukcję opracowano na podstawie:

1) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz.1182 z późn. zm.),
2) 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),
3) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r. Poz. 526).

II. Definicje

§ 1

1. Ilekroć w instrukcji jest mowa o:
   1) ustawie – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz.1182 z późn. zm.),
   2) rozporządzeniu – rozumie się przez to rozporządzenie 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),
   3) ZDKiUM – należy przez to rozumieć Zarząd Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu,
   4) administratorze danych – należy przez to rozumieć Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu,
   5) administratorze bezpieczeństwa informacji – należy przez to rozumieć osobę upoważnioną przez administratora danych osobowych, odpowiedzialną za bezpieczeństwo danych osobowych
   6) administratorze systemu informatycznego – należy przez to rozumieć zewnętrzną firmę informatyczną posiadającą upoważnienie administratora danych do administrowania zasobami danych ZDKiUM oraz nadzoru nad poprawnością stosowanych procedur zabezpieczenia danych,
   7) osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia lub innej umowy, osobę odbywającą u administratora danych staż absolwencki, praktykę studencką, wolontariat, której nadane zostało przez administratora danych upoważnienie do przetwarzania danych osobowych,

8) użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym,
9) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych ZDKiUM wyłącznie do własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
10) systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,
11) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego administratora danych,
12) haśle – rozumie się przez to co najmniej ośmioznakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie, której nadano identyfikator użytkownika,
13) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą;
    b) osoby, upoważnionej do przetwarzania danych;
    c) przedstawiciela, o którym mowa w art. 31a ustawy;
    d) podmiotu, o którym mowa w art. 31 ustawy;
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane;
13) serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.

III. Poziom bezpieczeństwa

§ 2

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, w którym urządzenia służące do przetwarzania danych osobowych są połączone z siecią publiczną, wprowadza się „wysoki" poziom bezpieczeństwa w rozumieniu § 6 rozporządzenia.

IV. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

§ 3

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz.1182 z późn. zm.), niniejszą instrukcją oraz posiadać upoważnienie do przetwarzania danych osobowych.

§ 4

1. Administrator systemu informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, wzór wniosku stanowi załącznik nr 1, z wyłączeniem osób kierujących ZDKiUM.

2. Wypełniony i podpisany wniosek o nadanie upewnień bezpośredni przełożony pracownika składa u administratora bezpieczeństwa informacji, który jest przekazywany do administratora systemu informatycznego.

3. Rejestracja użytkownika, polega na nadaniu unikalnego identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

4. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje administrator systemu informatycznego na wniosek przełożonego, załącznik nr 1, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.

5. Wyrejestrowanie, o którym mowa w ust. 3, może mieć charakter czasowy lub trwały.

6. Wyrejestrowanie następuje przez:
1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

6. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
1) wypowiedzenie umowy o pracę;
2) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych;
3) zawieszenie w pełnieniu obowiązków służbowych.

7. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego użytkownik był zatrudniony.

8. 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.

§ 5

1. Administrator systemu informatycznego zobowiązany jest do prowadzenia oraz ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym, wzór rejestru stanowi załącznik nr 2.

V. Metody i środki uwierzytelniania oraz procedury związane z ich zarządzeniem i użytkowaniem

§ 6

1. Identyfikator składa się z pierwszej litery imienia użytkownika i nazwiska pisanych małymi literami. W identyfikatorze pomija się polskie znaki diakrytyczne.

2. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu nadaje inny identyfikator odstępując od zasady określonej w ust. 1.

§ 7

1. W systemie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

2. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.

§ 8

1. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować administratora bezpieczeństwa informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.

§ 9

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

2. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni.

§ 10

1. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

§ 11

1. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
2. Hasła użytkowników utrzymuje się również w tajemnicy po upływie ich ważności.
3. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
4. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do powiadomienia administratora systemu w celu nadania nowego hasła.
5. Hasło powinno składać się z niepowtarzalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne o ile system informatyczny na to pozwala. Hasło nie może być identyczne z identyfikatorem użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.), ani z jego imieniem lub nazwiskiem.
6. Zakazuje się stosowania haseł, które użytkownik stosował uprzednio w okresie minionego roku, imion osób z najbliższej rodziny, ogólnie dostępnych informacji o użytkowniku takich jak numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, przewidywanych sekwencji z klawiatury (np.: „QWERTY" i „12345" itp.).
7. Zmiany hasła nie wolno zlecać innym osobom, oprócz administratora systemu.
8. Nie należy korzystać opcji zapamiętywania hasła w systemie.

§ 12

1. Hasło administratora systemu przechowywane jest w zamkniętej kopercie w szafie pancernej , do którego mają dostęp wyłącznie dyrektor oraz administrator bezpieczeństwa informacji.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 13

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie (w przypadku posiadania listwy), włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu identyfikatora indywidualnego oraz hasła identyfikatora znanego tylko użytkownikowi.

§ 14

1. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo administratora bezpieczeństwa informacji.

§ 15

1. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach,

§ 16

1. Monitory komputerów wyposażone są w włączające się po 5 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła,

§ 17

1. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest wylogować się z systemu lub w inny sposób zablokować stację robocza.

§ 18

1. Obowiązuje zakaz robienia kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez administratora systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.

§ 19

1. Jednostkowe dane mogą być przekazywane pocztą elektroniczną między komputerami administratora danych a komputerami przenośnymi użytkowników tylko po ich zabezpieczeniu hasłem.

§ 20

1. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wypisów.

§ 21

1. Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak aby zapobiegać ich utracie,

§ 22

1. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych programów, a następnie prawidłowym zamknięciu uruchomionych aplikacji, wylogowaniu się użytkownika, wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie (jeżeli jest podłączona),

§ 23

1. Przed opuszczeniem pokoju należy:
   1) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
   2) schować do zamykanych na klucz szaf akta zawierające dane osobowe,
   3) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
   4) zamknąć okna;

§ 24

1. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz.

§ 25

1. Jeśli niemożliwe jest umieszczenie wszystkich zawierających dane osobowe dokumentów w zamykanych szafach, to należy powiadomić o tym Kierownika Działu Organizacji, Zarządzania i Kadr, który zgłasza osobom sprzątającym jednorazową rezygnację z wykonania usługi sprzątania.

§ 26

1. Jeżeli jest to możliwe, to przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji dotyczące pracy na komputerach stacjonarnych.

§ 27

1. Użytkownicy, którym zostały powierzone komputery przenośne powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych; szczególną ostrożność należy zachować podczas ich transportu.

§ 28

1. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

§ 29

1. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.

2. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż co 30 dni.

§ 30

1. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub obszernych z nich wypisów.

§ 31

1. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach stacjonarnych oraz przenośnych.

2. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu informatycznego, stosownie do wymagań niniejszej instrukcji.

3. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to administratorowi systemu.

§ 32

1. Komputery stacjonarne oraz przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizacja pobierana jest automatyczne lub przez administratora systemu.

VIII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków ich kopii zapasowych

§ 33

1. Elektroniczne nośniki informacji:
   1) Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę ZDKiUM.
   2) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych.
   3) Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
   4) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe uszkadza się je w sposób mechaniczny uniemożliwiając ich odczytanie.
   5) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych.
   6) 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.

§ 34

1. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną.

§ 35

1. Na nośnikach, o których mowa w § 34, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.

§ 36

1. W przypadku posługiwania się nośnikami danych pochodzących od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.

§ 37

1. Nośniki magnetyczne z jednostkowymi danymi osobowymi są, na czas ich użyteczności, przechowywane w zamkniętych na klucz szafach, a po ich wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

§ 38

1. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

§ 39

1. Kopie zapasowe programów, których przydatność nie nadaje się do dalszego wykorzystania są trwale niszczone mechanicznie w niszczarce.

§ 40

1. Kopie zapasowe:
   1) Kopie bezpieczeństwa są przechowywane w szafie metalowej w pokoju Działu Organizacji Zarządzania i Kadr w budynku ZDKiUM.
   2) Dostęp do danych opisanych w pkt 1 ma administrator systemu informatycznego.

§ 41

1. Wydruki:
   1) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
   2) Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
   3) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

IX. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed wirusami komputerowymi

§ 42

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora (ciągła praca w tle).

2. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.

3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.

4. Jeżeli oprogramowanie antywirusowe pozwala, to należy ustawić harmonogram zadań tak, aby raz w tygodniu lub więcej razy sprawdzał daną jednostkę komputerową pod kątem obecności wirusów.

5. Do obowiązków administratora systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.

§ 43

1. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym.
2. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.

§ 44

1. Zabrania się pobierania z internetu plików niewiadomego pochodzenia.
2. Każdy plik pobrany z internetu musi być sprawdzony programem antywirusowym.
3. Sprawdzenia dokonuje użytkownik, który pobrał plik.

§ 45

1. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.

2. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

§ 46

1. Administrator systemu informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co trzy miesiące.

2. Kontrola antywirusowa przeprowadzana jest również w przypadku stwierdzenia nieprawidłowości, zgłoszonych przez pracownika, w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

§ 47

1. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.

§ 48

1. Użytkownik obowiązany jest zawiadomić administratora systemu o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

§ 49

1. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

X. Kontrola nad wprowadzaniem, przetwarzaniem i udostępnianiem danych osobowych

§ 50

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.

§ 51

1. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

§ 52

1. Aplikacje danych osobowych do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych.

2. Zakres informacji powinien obejmować co najmniej dane odbiorcy, datę wydania, zakres udostępnionych danych.

XI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 53

1. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.

2. Przeglądy i konserwacje urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

3. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny powinny być przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić administratora bezpieczeństwa informacji.

§ 54

1. Przeglądu pliku zawierającego raport dotyczący działalność aplikacji bądź systemów serwerowych (log systemowy) administrator systemu dokonuje nie rzadziej niż raz na miesiąc.

2. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale administratora systemu nie rzadziej niż raz na miesiąc.

§ 55

1. W przypadku działań konserwacyjnych, awarii oraz napraw administrator systemu informatycznego prowadzi „Dziennik systemu informatycznego Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu" załącznik nr 3.

2. Wpisów w dzienniku może dokonywać administrator danych, administrator bezpieczeństwa informacji.

XII. Naprawa urządzeń komputerowych z chronionymi danymi osobowymi

§ 56

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych przeprowadzane są , jeżeli jest to możliwe, przez administratora systemu.

2. Naprawy i zmiany w systemie informatycznym administratora danych przeprowadzane przez serwisanta prowadzone są pod nadzorem administratora systemu, jeżeli jest to możliwe, w siedzibie administratora danych lub poza siedzibą administratora danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

XIII. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

§ 57

1. Użytkownik zobowiązany jest zawiadomić administratora bezpieczeństwa informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła),
2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
4) wykryciu wirusa komputerowego,
5) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego administratora danych,
6) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
7) zmianie położenia sprzętu komputerowego,
8) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

§ 58

1. Do czasu przybycia na miejsce administratora bezpieczeństwa informacji:

1) jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia a następnie uwzględnić w działaniu ustalenie jego przyczyny lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
5) przygotować opis incydentu,
6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji.

2. Administrator bezpieczeństwa informacji po otrzymaniu zawiadomienia, o którym mowa w § 57, powinien niezwłocznie:

1) przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
2) podjąć działania chroniące system przed ponownym naruszeniem,
3) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego administratora danych, a następnie niezwłocznie przekazać jego kopie administratorowi danych.

§ 59

1. Administrator bezpieczeństwa informacji może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

§ 60

1. W razie odtwarzania danych z kopii zapasowych Administrator systemu obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu; dotyczy to zwłaszcza przypadków infekcji wirusowej.

§ 61

1. Administrator danych po zapoznaniu się z raportem, o którym mowa w § 58 ust. 2 pkt 3, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych bądź zastosowaniu środków ochrony fizycznej.

§ 62

1. Administrator bezpieczeństwa informacji zobowiązany jest do informowania administratora danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

§ 63

1. Administrator bezpieczeństwa informacji składa raz w roku administratorowi danych kompleksową analizę zarządzania systemem informatycznym.

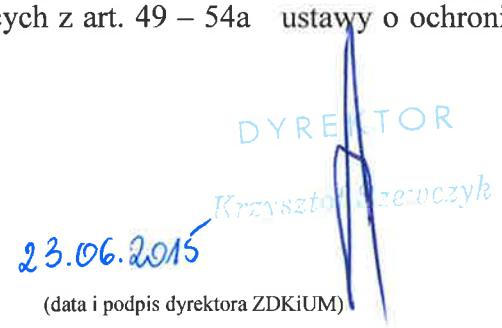
XIV. Postanowienia końcowe

§ 64

1. W sprawach nieuregulowanych w niniejszej instrukcji należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

§ 65

1. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, wynikających z art. 49 – 54a ustawy o ochronie danych osobowych.



23.06.2015

(data i podpis dyrektora ZDKiUM)

Załącznik nr 1
do Instrukcji zarządzania systemem informatycznym
w Zarządzie Dróg Komunikacji i Utrzymania Miasta
w Wałbrzychu

WNIOSEK
O NADANIE / ODEBRANIE* UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	**Wydział / samodzielne stanowisko**

Opis i zakres uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
Podpis administratora systemu:	Akceptacja administratora bezpieczeństwa informacji:

* niepotrzebne skreślić

Załącznik nr 2
do Instrukcji zarządzania systemem informatycznym
w Zarządzie Dróg Komunikacji i Utrzymania Miasta
w Wałbrzychu

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNINYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika

Załącznik nr 3
do Instrukcji zarządzania systemem informatycznym
w Zarządzie Dróg Komunikacji i Utrzymania Miasta
w Wałbrzychu

DZIENNIK SYSTEMU INFORMATYCZNEGO
ZARZĄDU DRÓG, KOMUNIKACJI I UTRZYMANIA MIASTA W WAŁBRZYCHU

L.p.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:

1) w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
2) w przypadku konserwacji systemu – opis podjętych działań, wnioski.