ZARZĄD GEODEZJI, KARTOGRAFII
I KATASTRU MIEJSKIEGO we Wrocławiu
al. Marcina Kromera 44, 51-163 Wrocław

00000001

ZARZĄDZENIE NR 13/2017

Dyrektora Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu
z dnia 29 marca 2017r.

w sprawie wprowadzenia Polityki Bezpieczeństwa w ZGKiKM

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016, poz. 922 z późn. zm.) oraz §3, §4 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), ustala się następujące wytyczne polityki bezpieczeństwa danych osobowych przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego w związku z realizacją celów statutowych jednostki organizacyjnej Gminy Wrocław, nie posiadającej osobowości prawnej i działającej w formie jednostki budżetowej zgodnie z postanowieniami uchwały Nr XI/383/99 Rady Miejskiej Wrocławia z dnia 8 lipca 1999 r. w sprawie przekształcenia zakładu budżetowego Gminy Wrocław o nazwie „Zarząd Geodezji, Kartografii i Katastru Miejskiego" w jednostkę budżetową (Biuletyn Urzędowy Rady Miejskiej Wrocławia Nr 7, poz. 340), oraz §16 ust. 1 Regulaminu Organizacyjnego Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu, zarządzam co następuje:

PREAMBUŁA

§1

W celu podkreślenia nieodzowności przestrzegania zasad ochrony danych osobowych przetwarzanych przez Zarząd Geodezji, Kartografii i Katastru Miejskiego przy użyciu metod tradycyjnych i elektronicznych, ustanawiamy niniejszy dokument jako podstawę standardu w zakresie bezpieczeństwa tych danych. Dokument ten stanowi integralną cześć zasad bezpieczeństwa odnoszących się do wszelkich przetwarzanych przez Zarząd Geodezji, Kartografii i Katastru Miejskiegoinformacji, jeśli jednak ustanowione standardy ogólne nie zapewniałyby identycznego lub wyższego stopnia bezpieczeństwa, należy traktować go jako nadrzędny dokument w stosunku do innych dokumentów z zakresu bezpieczeństwa informacji.

§2

Ustala się zasady ochrony danych osobowych przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu, obejmujące:

1) Politykę bezpieczeństwa informacji – stanowiącą załącznik nr 1 do zarządzenia;
2) Instrukcję zarządzania systemem informatycznym – stanowiącą załącznik nr 2 do zarządzenia.

GMINA WROCŁAW
pl. Nowy Targ 1-8
50-141 Wrocław
Z-CA PREZYDENTA
Dorota Olearnik
Z-ca DYREKTORA WYDZIAŁU
ZARZĄDZANIA FUNDUSZAMI

ZARZĄD GEODEZJI, KARTOGRAFII
I KATASTRU MIEJSKIEGO we Wrocławiu
al. Marcina Kromera 44, 51-163 Wrocław
tel. 71 32 72 100, fax 71 32 72 350

Za zgodność z oryginałem
22-05-2017
Wrocław, dnia.....
od str. 1 do 46
DYREKTOR
Anna Głuch

§3

W celu efektywnej ochrony danych osobowych administrowanych przez Administratorów Danych Osobowych określonych w dokumentach, o których mowa w §2 niniejszego zarządzenia, wszyscy pracownicy zobowiązani są do zapoznania się z zasadami wynikającymi z niniejszego dokumentu oraz do stosowania procedur i zasad z niego wynikających.

§4

1. Z dniem wejścia w życie niniejszego zarządzenia tracą moc:
   1) Zarządzenie nr 17/2009z dnia 29.05.2009 w sprawie wprowadzenia w życie „Zasad i procedur udostępniania i ochrony informacji w ZGKiKM,
   2) Zarządzenie nr 13/99 z dnia 30.09.1999 w sprawie wprowadzenia w życie „Instrukcji zasad posługiwania się w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu systemem informatycznym wprzetwarzaniu danych osobowych",
   3) Zarządzenie nr 36/20017 z dnia 17.12.2007r. w sprawie zmiany Zarządzenia nr 13/99.
   4) Traci moc Zarządzenie nr 30/2016 z dnia 31.10.2016 w sprawie wprowadzenia w życie Regulaminu korzystania z usługi IP VPN.
2. Zarządzenie wchodzi w życie z dniem podpisania

DYREKTOR
Anna Głuch

RADCA PRAWNY
Aleksandra Przyjoda-Szyszka

Załącznik nr 1
do Zarządzenia nr 13/2017 z dnia 29.03.2017 r.
Dyrektora Zarządu Geodezji, Kartografii
i Katastru Miejskiego we Wrocławiu

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Rozdział 1.
POSTANOWIENIA OGÓLNE

§1

1. Polityka bezpieczeństwa informacji stanowi zestaw praw i reguł określających sposób zarządzania, ochrony i przetwarzania informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiego.
2. Polityka bezpieczeństwa informacji jest dokumentem określającym zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorach danych:
   1) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych;
   2) w dokumentach, rejestrach, kartotekach, księgach, wykazach, skorowidzach i innych zbiorach ewidencyjnych.
3. Ochrona danych osobowych obowiązuje wszystkich pracowników Zarządu Geodezji, Kartografii i Katastru Miejskiego, którzy mają dostęp do informacji przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego, bez względu na zajmowane stanowisko, miejsce wykonywania pracy, jak również rodzaj stosunku pracy.
4. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
5. Administrator Danych jest odpowiedzialny za wdrożenie i interpretację Polityki bezpieczeństwa informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiegooraz opracowanie procedur w zakresie przetwarzania danych osobowych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego.
6. Polecenia osób delegowanych w zakresie ochrony danych osobowych, wyznaczonych przez Administratora Danych, do działań w zakresie ochrony danych osobowych w Zarządzie Geodezji, Kartografii i Katastru Miejskiegomuszą być bezwzględnie wykonywane przez wszystkich pracowników.
7. Gromadzenie i przetwarzanie danych osobowych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego jest dopuszczalne wyłącznie w zakresie niezbędnym do wykonywania zadań Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu.
8. Wszyscy pracownicy Zarządzie Geodezji, Kartografii i Katastru Miejskiego, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

§ 2

Użyte w Polityce określenia oznaczają:
1) **ZGKiKM** – Zarząd Geodezji, Kartografii i Katastru Miejskiego;
2) **komórka organizacyjna** – właściwy rzeczowo biuro, dział, którego zadania określone zostały w Regulaminie organizacyjnym Zarządu Geodezji, Kartografii i Katastru Miejskiego – Zarządzenie 26/2014 z dnia 28 sierpnia 2014 r.
3) **Regulamin organizacyjny** – regulamin, o którym mowa w pkt 2;

4) **Regulamin pracy** – Zarządzenie nr 14/2009 w sprawie wprowadzenia w życie Regulaminu Pracy Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu;
5) **Polityka** – Polityka bezpieczeństwa informacji obowiązująca w ZGKiKM;
6) **Instrukcja** – Instrukcja zarządzania systemem informatycznym ZGKiKM;
7) **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2016 r., poz. 922)
8) **rozporządzenie** – 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);
9) **Administrator Danych (AD)**:
a) Zarząd Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu w zakresie danych osobowych pracowników oraz danych osobowych pozyskanych w ramach bieżącej działalności jednostki, z wyłączeniem danych przetwarzanych przez pozostałych zdefiniowanych w niniejszym akcie wewnętrznym Administratorów Danych,
b) Prezydent Wrocławia, w imieniu którego działa upoważniony Geodeta Miejski – w zakresie danych osobowych przetwarzanych jako organ w związku z realizacją zadań z art. 7d ustawy Prawo Geodezyjne i Kartograficzne,
c) Dyrektor Zarządu, Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu – w zakresie danych osobowych przetwarzanych jako organ przeprowadzający postępowania podziałowe z ustawy o Gospodarce Nieruchomościami oraz postępowania rozgraniczeniowe z ustawy Prawo Geodezyjne i Kartograficzne.
10) **Administrator Bezpieczeństwa Informacji (ABI)** – pracownik ZGKiKM wyznaczony przez Administratora Danych, nadzorujący i kontrolujący przestrzeganie zasad ochrony danych osobowych w ZGKiKM;
11) **Administrator Systemu Informatycznego (ASI)** – pracownik ZGKiKM wyznaczony przez Administratora Danych, nadzorujący i kontrolujący funkcjonowanie całości systemu informatycznego ZGKiKM, w szczególności części systemu, w których przetwarzane są dane osobowe;
12) **Administrator Systemu** – specjalista informatyk, realizujący zadania techniczne w celu zapewnienia bezpiecznej eksploatacji wybranych urządzeń i aplikacji wykorzystywanych do przetwarzania danych;
13) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
17) **naruszenie zabezpieczenia** –jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności informacji;
18) **dostępność informacji** – zapewnienie, że podmioty uprawnione uzyskują dostęp do informacji tylko w uzasadnionych przypadkach;
19) **nośnik** – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi;
20) **zniszczenie nośnika** – trwałe i nieodwracalne fizyczne zniszczenie nośnika uniemożliwiające rekonstrukcję i odzyskanie danych;
21) **Generalny Inspektor Ochrony Danych Osobowych (GIODO)** – organ do spraw ochrony danych osobowych działający na podstawie ustawy;

22) **pracownik** – osoba, która świadczy pracę na rzecz ZGKiKM, bez względu na jakiej podstawie (w tym umowa zlecenia, staż, praktyki);
23) **użytkownik** – osoba przetwarzająca dane, w tym dane osobowe, w systemie informatycznym, w ramach wykonywanych zadań, niezależnie od charakteru zatrudnienia lub wykonywanych prac zleconych.

Rozdział 2.
CEL I ZAKRES STOSOWANIA

§3

1. Celem Polityki jest określenie postępowania gwarantującego bezpieczeństwo informacji przetwarzanych w ZGKiKM, w tym zabezpieczenie przetwarzanych przez ZGKiKM danych osobowych, poprzez podejmowanie działań mających na celu zapewnienie ich poufności, integralności, dostępności i rozliczalności.
2. Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych osobowych, przetwarzanych w ZGKiKM, zarówno w formie elektronicznej jak i papierowej.

§4

1. Obszar, w ramach którego przetwarzane są informacje, w tym dane osobowe, obejmuje budynek ZGKiKM położony we Wrocławiu przy al. Marcina Kromera44.
2. Obszar, o którym mowa w ust. 1 obejmuje również budynki i pomieszczenia podmiotów zewnętrznych, którym na podstawie zawartych umów powierzono przetwarzanie danych osobowych, w zakresie niezbędnym do wykonywania zadań dla ZGKiKM.

Rozdział 3.
SYSTEM OCHRONY DANYCH OSOBOWYCH

§5

Politykę stosuje się do zbiorów danych przetwarzanych w ZGKiKM.

§6

1. Szczegółowy wykaz budynków, tworzących obszar, w którym przetwarzane są dane osobowe wraz z programami zastosowanymi do ich przetwarzania zawarte są w dokumencie *Wykaz zbiorów danych osobowych przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego,* stworzonym według wzoru stanowiącego załącznik nr 6 do Polityki.
2. Wykaz o którym mowa w ust. 1 znajduje się u Administratora Bezpieczeństwa Informacji (ABI).
3. Opis struktury zbiorów danych, wskazujący na zawartość poszczególnych pól informacyjnych i powiązania między nimi, jest udostępniany przez Administratora Systemu Informatycznego (ASI).

§ 7

O celach i środkach przetwarzania danych osobowych w ZGKiKM decyduje Administrator Danych (AD).

§ 8

1. W celu nadzoru nad przestrzeganiem zasad ochrony danych osobowych w ZGKiKM, Administrator Danych (AD) wyznacza Administratora Bezpieczeństwa Informacji (ABI).
2. W celu nadzoru nad systemem informatycznym ZGKiKM, Administrator Danych(AD) wyznacza Administratora Systemu Informatycznego (ASI).

§ 9

Nadzór nad zbiorami danych osobowych w komórkach organizacyjnych sprawują Kierownicytych komórek.

Rozdział 4.
PRZETWARZANIE DANYCH OSOBOWYCH

§10

Dane osobowe przetwarzane w ZGKiKM podlegają ochronie zgodnie z przepisami ustawy.

§11

Przetwarzanie danych osobowych w ZGKiKM jest dopuszczalne wyłącznie w zakresie określonym w upoważnieniu do przetwarzania danych osobowych.

§12

Przetwarzanie danych osobowych nie może naruszać praw i wolności osób, których dane osobowe dotyczą. W szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§13

W przypadku zbierania jakichkolwiek danych osobowych, mających charakter dobrowolny, a zatem niewynikających z realizacji obowiązków ujętych w przepisach prawa, a w szczególności z przepisów kodeksu pracy, na potrzeby ZGKiKM bezpośrednio od osoby, której dane dotyczą, pracownik zbierający dane osobowe jest zobowiązany do przekazania tej osobie informacji o przysługujących jej prawach, w szczególności o:
1) pełnej nazwie i adresie siedziby Administratora Danych (AD);
2) celu zbierania danych osobowych;
3) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
4) dobrowolności podania danych osobowych lub obowiązku podania danych, a jeśli taki obowiązek istnieje, o jego podstawie prawnej.

§14

Każdej osobie, której dane osobowe są przetwarzane w ZGKiKM przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:
1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych (AD);
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§15

Na wniosek osoby, której dane osobowe dotyczą, Administrator Bezpieczeństwa Informacji (ABI) jest zobowiązany, w terminie do 30 dni od dnia wpłynięcia wniosku, wskazać w powszechnie zrozumiałej formie:
1) zakres przetwarzanych danych osobowych wnioskodawcy;
2) sposób pozyskania danych;
3) cel przetwarzania danych;
4) termin rozpoczęcia przetwarzania danych;
5) odbiorców oraz zakres udostępnienia danych.

§16

W razie wykazania przez osobę, której dane dotyczą, że jej dane osobowe, przetwarzane w ZGKiKM są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy Administrator Bezpieczeństwa Informacji (ABI) jest zobowiązany do uzupełnienia, uaktualnienia, sprostowania danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane osobowe dotyczą.

§17

1. Do przetwarzania danych osobowych w ZGKiKM mogą być dopuszczeni jedynie pracownicy posiadający pisemne upoważnienie wydane przez Administratora Danych (AD).
2. Pracownik ZGKiKM, przed dopuszczeniem go do przetwarzania danych osobowych, jest zobowiązany do zapoznania się z przepisami i procedurami dotyczącymi ochrony danych osobowych.

§18

Dostęp do danych osobowych, przetwarzanych w ZGKiKM, osoby niebędącej pracownikiem ZGKiKM, jest możliwy po uzyskaniu pozytywnej opinii Administratora Bezpieczeństwa Informacji (ABI), na podstawie pisemnego upoważnienia wydanego przez Administratora Danych (AD) oraz podpisaniu przez taką osobę oświadczenia o poufności. Wzór oświadczenia stanowi załącznik nr 5do Polityki.

Rozdział 5.
DOSTĘP PODMIOTÓW ZEWNĘTRZNYCH

§19

Celem procedury jest zapewnienie bezpieczeństwa informacji, w szczególności danych osobowych, udostępnionych lub powierzonych do przetwarzania przez ZGKiKM podmiotom zewnętrznym.

§ 20

1. Przetwarzanie danych osobowych zgromadzonych w ZGKiKM może zostać powierzone podmiotowi zewnętrznemu, wyłącznie w zakresie określonym w § 1 ust. 7, pod warunkiem zawarcia z tym podmiotem pisemnej umowy, w pełni uwzględniającej przepisy ustawy, rozporządzenia oraz wewnętrzne procedury ZGKiKM.
2. Zawarcie umowy, o której mowa w ust. 1, wymaga uzyskania pozytywnej opinii Administratora Bezpieczeństwa Informacji (ABI) oraz zgody Administratora Danych (AD).
3. Postanowienia umowy, o której mowa w ust. 1 zobowiązują podmiot zewnętrzny, któremu powierzono przetwarzanie danych osobowych min. do:
1) przetwarzania danych zgodnie z celem i zakresem określonym w umowie i niepoddawanie dalszemu przetwarzaniu niezgodnemu z celem;

2) przechowywanie danych nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
3) zastosowania, przed rozpoczęciem przetwarzania danych, zabezpieczeń określonych w rozporządzeniu.

§21

1. Udostępnianie podmiotom zewnętrznym danych osobowych przetwarzanych w ZGKiKM może się odbywać wyłącznie w trybie określonym w ustawie i procedurach wewnętrznych.
2. Każdorazowe udostępnienie podmiotowi zewnętrznemu danych osobowych przetwarzanych w ZGKiKM wymaga pozytywnej opinii Administratora Bezpieczeństwa Informacji (ABI) oraz zgody Administratora Danych (AD).
3. Dane osobowe przetwarzane w ZGKiKM udostępnia się na pisemny umotywowany wniosek, chyba, że przepisy odrębne stanowią inaczej.

§22

1. Administrator Bezpieczeństwa Informacji (ABI) prowadzi Rejestr podmiotów zewnętrznych, którym powierzono przetwarzanie danych osobowych.
2. Administrator Bezpieczeństwa Informacji (ABI) prowadzi Rejestr podmiotów zewnętrznych, którym udostępniono dane osobowe.

§23

1. Rejestry, o których mowa w § 22 zawierają:
1) datę powierzenia/udostępnienia informacji;
2) adresata powierzonych/udostępnionych danych;
3) zakres powierzonych/udostępnionych danych.
2. Ewidencjonowanie następuje bezpośrednio po powierzeniu lub udostępnieniu danych osobowych.

§ 24

Dane udostępniane ZGKiKM przez podmiot zewnętrzny wykorzystywane są zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Rozdział 6.
OBOWIĄZKI I UPRAWNIENIA W SYSTEMIE OCHRONY DANYCH OSOBOWYCH

§ 25

1. **Administrator Danych** (AD) jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające odpowiednią do zagrożeń oraz kategorii danych ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Do zadań Administratora Danych (AD) należy:
1) zatwierdzanie procedur regulujących postępowanie przy przetwarzaniu danych osobowych w ZGKiKM;
2) nadawanie osobom upoważnień do przetwarzania danych osobowych w zakresie, o którym mowa w § 1 ust. 7;
3) wyznaczenie Administratora Bezpieczeństwa Informacji (ABI);
4) wyznaczenie Administratora Systemu Informatycznego (ASI);

5) współpraca z Generalnym Inspektorem Ochrony Danych Osobowych (GIODO), w tym zgłaszanie Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO) zbiorów danych osobowych ZGKiKM podlegających rejestracji;
6)podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia zabezpieczenia danych osobowych;
7) parafowaniu projektów umów w zakresie powierzania przetwarzania danych osobowych podmiotom zewnętrznym;
8) inicjowaniu szkoleń pracowników ZGKiKM z obowiązujących przepisów w zakresie ochrony danych osobowych.

§ 26

1. **Administrator Bezpieczeństwa Informacji** (ABI) wdraża i nadzoruje przestrzeganie zasad ochrony danych osobowych w ZGKiKM.
2. Do zadań Administratora Bezpieczeństwa Informacji (ABI) należy:
1) współdziałanie z Administratorem Danych (AD) w zakresie zapewniającym wypełnianie obowiązków wynikających z ustawy i rozporządzenia oraz przepisów wewnętrznych ZGKiKM;
2) sprawowanie nadzoru nad wdrożeniem stosownych środków organizacyjno-technicznych w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w ZGKiKM;
3) aktualizacja i dostosowanie Polityki i Instrukcji do wymogów wynikających z przepisów prawa;
4) prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania danych osobowych w ZGKiKM;
5) przygotowywanie projektów upoważnień do przetwarzania danych osobowych w ZGKiKM i przedkładanie ich Administratorowi Danych (AD) do zatwierdzenia;
6) prowadzenie i aktualizacja wykazu zbiorów danych osobowych ZGKiKM, oprogramowania używanego do ich przetwarzania oraz budynków, tworzących obszar, w obrębie którego przetwarzane są dane osobowe, zawartych w *Wykazie zbiorów danych osobowych przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego*oraz tworzenia opisów tych zbiorów;
7) prowadzenie rejestrów, o których mowa w § 22 Polityki;
8) prowadzenie rejestru stwierdzonych naruszeń, którego wzór stanowi załącznik nr 7 do Polityki;
9) identyfikacja zagrożeń i analiza ryzyka, w odniesieniu do procesu przetwarzania danych osobowych w ZGKiKM oraz informowanie o wynikach analizy Administratora Danych (AD);
10) wykrywanie naruszeń i właściwe reagowanie w sytuacji naruszenia lub podejrzenia naruszenia zasad ochrony danych osobowych;
11) informowanie osób uprawnionych o przysługujących im prawach oraz udzielanie informacji w zakresie ochrony danych osobowych;
12) przeprowadzanie audytu systemu ochrony danych osobowych oraz informowanie o wynikach audytu Administratora Danych (AD) w formie pisemnego sprawozdania.

§ 27

1. **Administrator Systemu Informatycznego** (ASI) zarządza systemami informatycznymi służącymi do przetwarzania danych osobowych oraz pełni nadzór nad ich zabezpieczeniem;
2. Do zadań Administratora Systemu Informatycznego (ASI) należy:
1) prowadzenie bieżącej kontroli oraz dokonywanie oceny stanu bezpieczeństwa systemu informatycznego ZGKiKM oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;

2) prowadzenie dokumentacji dotyczącej naruszeń zabezpieczeń systemu informatycznego ZGKiKM;
3) nadzór nad wykorzystywanym w ZGKiKM oprogramowaniem pod względem jego legalności;
4) aktualizacja wykorzystywanego w ZGKiKM oprogramowania;
5) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe;
6) wykonywanie kopii zapasowych, ich przechowywanie oraz ich okresowe sprawdzanie pod kątem dalszej przydatności;
7) koordynowanie pracy Administratorów Systemu;
8) inicjowanie i podejmowanie przedsięwzięć w zakresie poprawy bezpieczeństwa ochrony danych osobowych w systemie informatycznym;
9) prowadzenie następujących rejestrów, związanych z funkcjonowaniem systemu informatycznego ZGKiKM:
a) rejestru kontroli stanowisk użytkowników,
b) rejestru kopii zapasowych systemów informatycznych,
c) rejestru kontroli stanu zabezpieczenia systemów informatycznych, rejestru zmiany haseł administracyjnych.

§ 28

1. **Kierownik** komórki organizacyjnej nadzoruje przestrzeganie zasad bezpieczeństwa przy przetwarzaniu danych osobowych w zbiorach danych w podległej sobie komórce organizacyjnej.
2. Kierownik komórki organizacyjnej, na podstawie pisemnego upoważnienia do przetwarzania danych osobowych w zakresie zarządzania danymi w podległej mu komórce organizacyjnej, jest zobowiązany do:
1) określania obowiązków i uprawnień pracowników w zakresie przetwarzania danych osobowych;
2) wnioskowania do Administratora Bezpieczeństwa Informacji (ABI) o udzielenie, nadanie, zmianę lub odwołanie upoważnienia do przetwarzania danych osobowych podległym pracownikom. Wzór wniosku o udzielenie upoważnienia stanowi załącznik nr 3do Polityki;
3) wnioskowania do Administratora Systemu Informatycznego (ASI), po akceptacji Z-cy Dyrektora ds. Systemów Informatycznych, o przydzielenie nowemu pracownikowi komórki organizacyjnej dostępu do obszarów roboczych i systemu informatycznego ZGKiKM. Zgłoszenia dokonuje się za pomocą formularza informacyjnego, którego wzór stanowi załącznik nr 8do Polityki;
4) informowania Administratora Systemu Informatycznego (ASI) o wszelkich zmianach w zakresie danych personalnych, danych o zatrudnieniu oraz danych o dostępie do obszarów roboczych i systemu informatycznego ZGKiKM. Aktualizacji dokonuje się za pomocą formularza informacyjnego, o którym mowa w pkt 3;
5) stosowania środków organizacyjnych zalecanych przez Administratora Danych (AD) w celu zapewnienia ochrony przetwarzanych danych osobowych;
6) wykonywania zaleceń Administratora Bezpieczeństwa Informacji (ABI) w zakresie ochrony danych osobowych;
7) sprawowania nadzoru nad obiegiem oraz przechowywaniem dokumentów i nośników, zawierających dane osobowe;
8) zgłaszania Administratorowi Bezpieczeństwa Informacji (ABI) zbiorów danych osobowych przetwarzanych w komórce organizacyjnej w celu ich rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO), jeśli rejestracja jest wymagana;

9) zgłaszania Administratorowi Bezpieczeństwa Informacji (ABI) potrzeb szkoleniowych dla pracowników z przepisów obowiązujących w zakresie ochrony danych osobowych;
10) zgłaszania Administratorowi Bezpieczeństwa Informacji (ABI) wszelkich zmian dokonywanych w przetwarzanych w komórce organizacyjnej, zbiorach danych osobowych, w szczególności obejmujących rozszerzenie zakresu przetwarzanych danych;
11) zgłaszania Administratorowi Bezpieczeństwa Informacji (ABI) wszelkich przypadków świadczących o naruszeniu lub możliwości naruszenia postanowień Polityki i Instrukcji.

§ 29

Pracownicy ZGKiKM, upoważnieni do przetwarzania danych osobowych, są zobowiązani do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia, a także do:
1) zapoznania się oraz stosowania procedur obowiązujących w ZGKiKM w zakresie ochrony danych osobowych, w tym Polityki i Instrukcji;
2) przetwarzania danych osobowych wyłącznie w zakresie wskazanym w upoważnieniu do przetwarzania danych i w wyznaczonych do tego celu pomieszczeniach służbowych;
3) zabezpieczania danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
4) udzielania informacji związanych z przetwarzaniem oraz ochroną danych osobowych Administratorowi Bezpieczeństwa Informacji (ABI);
5) bezzwłocznego zawiadamiania Administratora Bezpieczeństwa Informacji (ABI) oraz kierownika komórki organizacyjnej o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych w ZGKiKM.

§ 30

W celu uzyskania dostępu do danych osobowych przetwarzanych w ZGKiKM pracownik jest zobowiązany do złożenia pisemnego oświadczenia o poufności, którego wzór stanowi załącznik nr 5do Polityki. Oświadczenie dołącza się do akt osobowych pracownika.

Rozdział 7.
UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 31

1. Przed otrzymaniem dostępu do danych osobowych oraz rozpoczęciem ich przetwarzania należy uzyskać stosowne upoważnienie wydane przez Administratora Danych (AD).
2. W upoważnieniu zawarty jest okres jego obowiązywania oraz zakres uprawnień dostępowych pracownika.

§ 32

1. Administrator Danych (AD) w drodze pisemnego upoważnienia ustanawia kierowników komórek organizacyjnych odpowiedzialnymi za nadzór nad prawidłowym przetwarzaniem danych osobowych w zakresie właściwych rzeczowo zbiorów danych.
2. Kierownikkomórki organizacyjnej składa do Administratora Bezpieczeństwa Informacji (ABI) wniosek o nadanie, zmianę lub cofnięcie upoważnienia do przetwarzania danych osobowych.
3. Na podstawie wniosku, o którym mowa w ust. 2, Administrator Danych (AD) nadaje osobie upoważnienie do przetwarzania danych osobowych.

§ 33

1. Administrator Bezpieczeństwa Informacji (ABI) prowadzi ewidencję pracowników posiadających upoważnienia do przetwarzania danych osobowych w ZGKiKM.
2. Rejestr upoważnień, o którym mowa w ust. 1, zawiera:
1) imię i nazwisko pracownika;
2) stanowisko;
3) identyfikator użytkownika w systemie informatycznym;
4) datę nadania uprawnień;
5) datę ustania uprawnień;
6)zakres przydzielonych uprawnień.
3. Upoważnienia, o których mowa w ust. 1, sporządza się w dwóch egzemplarzach, z których po jednym egzemplarzu otrzymują:
1) Administrator Bezpieczeństwa Informacji (ABI);
2) upoważniony pracownik.
4. Potwierdzone za zgodność z oryginałem kopie upoważnień, o których mowa w ust. 1, przekazywane są przez Administratora Bezpieczeństwa Informacji (ABI) do komórki kadrowej ZGKiKM, celem dołączenia do akt osobowych pracowników.

Rozdział 8.
TECHNICZNE I ORGANIZACYJNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

§ 34

Administrator Danych (AD) jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zapewniających bezpieczeństwo i ochronę przetwarzanych danych osobowych, bez względu na formę ich przetwarzania.

§ 35

W ZGKiKM stosuje się następujące systemy zabezpieczeń przed nieuprawnionym dostępem do danych osobowych:
1) Zabezpieczenia pomieszczeń, składających się na obszar przetwarzania danych osobowych:
a) w przypadku opuszczenia pomieszczenia, w którym przetwarza się dane osobowe, przez ostatnią osobę, pomieszczenie zamykane jest na klucz, także w godzinach pracy;
b) po godzinach pracy klucze do pomieszczeń, w których przetwarzane są dane osobowe, przechowywane są w we właściwej recepcji;
c) w pomieszczeniach , gdzie mogą przebywać osoby nieuprawnione do przetwarzania danych osobowych, dokumenty zawierające dane osobowe powinny być zabezpieczone przed ich nieuprawnionym dostępem.
d) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są niezwłocznie w niszczarkach;
e) budynek ZGKiKM nadzorowany jest przez pracowników ochrony przez całą dobę; budynek wyposażony jest w system alarmowy przeciwwłamaniowy;
f) uzyskanie dostępu do obszarów roboczych ZGKiKM możliwe jest jedynie za pomocą indywidualnej identyfikacyjnej karty magnetycznej;
g) dostęp do wyznaczonych pomieszczeń kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
2) Zabezpieczenia zbiorów danych osobowych w formie elektronicznej przed nieautoryzowanym dostępem:
a) identyfikacja użytkownika w systemie informatycznym wymaga zastosowania uwierzytelnienia;

b) niepowtarzalne indywidualne identyfikatory dla użytkowników systemu informatycznego;
c) udostępnianie użytkownikowi programów i baz danych, zawierających dane osobowe następuje na podstawie upoważnienia do przetwarzania danych osobowych, wydanego przez Administratora Danych (AD);
d) podłączenie urządzenia końcowego do sieci komputerowej ZGKiKM dokonywane jest przez Administratora Systemu Informatycznego (ASI) lub Administratora Systemu;
e) odseparowanie wewnętrznej sieci komputerowej ZGKiKM od sieci publicznej za pomocą urządzeń typu Firewall;
f) wyposażenie wszystkich stanowisk komputerowych w indywidualną ochronę antywirusową;
g) zabezpieczenie hasłami kont na komputerach oraz używanie kont z ograniczonymi uprawnieniami do ciągłej pracy;
h) automatyczne wygaszanie ekranu i blokowanie nieużywanego komputera po upływie określonego czasu;
i) wymuszanie okresowej zmiany hasła użytkownika co 30 dni;
j) ustawienie monitorów stanowisk komputerowych używanych do przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym;
k) udostępnianie kluczy i kart dostępu do serwerowni wyłącznie osobom do tego upoważnionym.
3) Zabezpieczenia danych osobowych przed utratą w wyniku awarii:
a) zastosowanie zasilaczy zapasowych UPS w celu ochrony strategicznych stanowisk komputerowych oraz serwerów przed skutkami zaniku zasilania;
b) cykliczne wykonywanie kopii zapasowych zgromadzonych danych, z których w przypadku awarii, odtwarzane są dane i system operacyjny;
c) zastosowanie klimatyzatorów w celu zapewnienia właściwej temperatury i wilgotności powietrza w serwerowniach;
d) rozmieszczenie gaśnic w serwerowniach.
4) Stały nadzór nad systemem stosowanych zabezpieczeń:
a) pracownicy ZGKiKM są zobowiązani do zwracania uwagi na prawidłowość pracy systemów informatycznych, przestrzegania wewnętrznych procedur bezpieczeństwa, informowania Administratora Bezpieczeństwa Informacji (ABI) oraz przełożonych o zauważonych lub potencjalnych nieprawidłowościach;
b) przetwarzanie danych dopuszczalne jest wyłącznie na zarejestrowanych stacjach roboczych, komputerach przenośnych oraz innych nośnikach informacji;
c) Administrator Bezpieczeństwa Informacji (ABI) przeprowadza audyt, o którym mowa w § 26 ust. 2 pkt 12.

§ 36

1. Uszkodzone lub wycofywane elektroniczne nośniki danych zawierające dane osobowe podlegają fizycznemu zniszczeniu. Każdorazowo sporządzany jest protokół zniszczenia.
2. Komputery podlegające naprawie przekazywane są do punktów serwisowych po wymontowaniu dysków twardych. Każdorazowo sporządzany jest protokół naprawy.

Rozdział 9.
KONTROLA NAD PRZESTRZEGANIEM OCHRONY DANYCH OSOBOWYCH

§ 37

Ogólny nadzór nad przetwarzaniem danych osobowych w ZGKiKM sprawuje Administrator Danych (AD).

§ 38

Administrator Bezpieczeństwa Informacji (ABI) wykonuje bieżącą kontrolę nad przestrzeganiem przez pracowników, wdrożonych w ZGKiKM środków bezpieczeństwa oraz postanowień wewnętrznych procedur w zakresie zasad przetwarzania danych osobowych.

§ 39

Administrator Systemu Informatycznego (ASI) wykonuje bieżącą kontrolę w celu zapewnienia sprawnego działania i bezpieczeństwa systemów informatycznych ZGKiKM.

§ 40

Przy realizacji kontroli, o których mowa w § 38 i 39 Administratorowi Bezpieczeństwa Informacji (ABI) oraz Administratorowi Systemu Informatycznego (ASI) przysługują uprawnienia do przeprowadzania czynności kontrolnych, w szczególności do:
1) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych lub przetwarzane są dane osobowe poza zbiorem danych;
2) prawo do przeprowadzenia inspekcji, oględzin urządzeń, nośników i systemów informatycznych;
3) prawo wglądu do dokumentów mających bezpośredni związek z przedmiotem kontroli i sporządzania ich kopii;
4) prawo do żądania wyjaśnień.

§ 41

1. Audyt w zakresie przestrzegania ochrony danych osobowych w ZGKiKM, o którym mowa w § 26 ust. 2 pkt 12 sporządzany jest za poprzedni rok kalendarzowy.
2. Administrator Bezpieczeństwa Informacji (ABI) do końca pierwszego kwartału każdego roku, sporządza sprawozdanie z audytu o którym mowa w ust 1.
3. Sprawozdanie, o którym mowa w ust. 2 zawiera również:
1) wnioski bieżących kontroli, o których mowa w § 38 i 39;
2) analizę zagrożeń i ryzyka w odniesieniu do procesu przetwarzania danych osobowych w ZGKiKM;
3) wnioski i zalecenia dotyczące funkcjonowania systemu ochrony danych osobowych w ZGKiKM.
4. Sprawozdanie, o którym mowa w ust. 2, Administrator Bezpieczeństwa Informacji (ABI) przedkłada Administratorowi Danych (AD).

Rozdział 10.
NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

§ 42

1. Poprzez naruszenie bezpieczeństwa danych osobowych należy rozumieć każdy stwierdzony przypadek nieuprawnionego dostępu lub ujawnienia danych osobowych nieupoważnionym do tego osobom.
2. Określa się tryb postępowania w przypadku:
1) naruszeń bezpieczeństwa danych osobowych.
2) naruszeń zabezpieczenia systemu informatycznego, w tym: stanu urządzeń, zawartości zbioru danych osobowych, ujawnienia sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej, mogących wskazywać na naruszenie zabezpieczeń tych danych.
3. Każdy pracownik ZGKiKM, posiadający upoważnienie do przetwarzania danych osobowych, jest odpowiedzialny za bezpieczeństwo tych danych.

4. Nadzór nad przestrzeganiem instrukcji postępowania w sytuacji naruszenia zasad ochrony danych osobowych sprawuje Administrator Bezpieczeństwa Informacji (ABI).

§ 43

Określa się następujący sposób postępowania w przypadku naruszenia ochrony danych osobowych:

1) każdy pracownik w momencie stwierdzenia naruszenia lub próby naruszenia bezpieczeństwa danych, obowiązany jest do niezwłocznego zawiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji (ABI) oraz Kierownikakomórki organizacyjnej;

2) w przypadku braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji (ABI) lub Kierownikakomórki organizacyjnej, należy:

a) jeśli taka możliwość istnieje, podjąć czynności zmierzające do zmniejszenia skutków zaistniałego naruszenia bezpieczeństwa,

b) jeśli mogłoby to przyczynić się do utrudnienia wyjaśnienia okoliczności zdarzenia, powstrzymać się od bieżącej pracy, w celu zabezpieczenia miejsca zdarzenia,

c) wstępnie udokumentować zaistniałe naruszenie bezpieczeństwa,

d) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji (ABI);

3) jeśli naruszeniu lub próbie naruszenia uległy dane w systemie informatycznym, dodatkowo powiadamiany jest Administrator Systemu Informatycznego (ASI);

4) Administrator Bezpieczeństwa Informacji (ABI) oraz, w przypadku naruszenia danych w systemie informatycznym, Administrator Systemu Informatycznego (ASI), po przyjęciu zawiadomienia dokumentują zaistniały przypadek naruszenia bezpieczeństwa danych oraz podejmują działania w celu wyjaśnienia sytuacji oraz usunięcia naruszenia, w szczególności:

a) dokonują szczegółowej analizy zaistniałej sytuacji, w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

b) podejmują odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieupoważnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych,

c) podejmują decyzję o celowości i potrzebie powiadomienia o naruszeniu bezpieczeństwa danych osobowych Administratora Danych (AD),

d) w przypadku potwierdzenia naruszenia bezpieczeństwa danych osobowych, dokonują identyfikacji rodzaju zaistniałego zdarzenia,

e) podejmują działania w celu przywrócenia prawidłowego stanu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną;

5) W ramach przyznanych uprawnień Administrator Bezpieczeństwa Informacji (ABI) oraz Administrator Systemu Informatycznego (ASI) mają prawo do:

a) żądania wyjaśnień od pracowników ZGKiKM,

b) nakazania przerwy w pracy w zakresie przetwarzania danych osobowych,

c) czasowego zablokowania uprawnień wskazanym użytkownikom lub wszystkim użytkownikom systemu informatycznego ZGKiKM;

6) Odmowa wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji (ABI) oraz z Administratorem Systemu Informatycznego (ASI), przy wyjaśnianiu okoliczności naruszenia zasad ochrony danych osobowych, będzie traktowana jako naruszenie obowiązków pracowniczych.

§ 44

1. Z przeprowadzonego postępowania Administrator Bezpieczeństwa Informacji (ABI), przy udziale Administratora Systemu Informatycznego (ASI) w przypadku naruszenia zabezpieczenia danych w systemie informatycznym, sporządza raport dla Administratora Danych (AD).
2. Raport powinien zawierać w szczególności: wskazanie osoby/osób powiadamiającej o naruszeniu lub możliwości naruszenia bezpieczeństwa oraz innych osób związanych ze zdarzeniem, okoliczności zdarzenia, rodzaj naruszenia, opis podjętych działań oraz ocenę przyczyn wystąpienia naruszenia, a także propozycje przedsięwzięć mających na celu naprawę powstałych szkód i zapobiegnięcie podobnym zdarzeniom w przyszłości.
3. Wobec pracowników, którzy dopuścili się naruszenia bezpieczeństwa danych osobowych lub zabezpieczeń systemu informatycznego stosuje się odpowiednie przepisy ustaw oraz postanowienia § 29 Regulaminu pracy, w zakresie odpowiedzialności dyscyplinarnej i porządkowej pracowników.

Rozdział 11.
POSTANOWIENIA KOŃCOWE

§ 45

1. Polityka jest dokumentem wewnętrznym i może być udostępniana uprawnionym podmiotom zewnętrznym w celu zapoznania się i postępowania w zgodzie z postanowieniami niniejszego dokumentu.
2. Do spraw nieuregulowanych w Polityce, w zakresie ochrony danych osobowych stosuje się przepisy ustawy, rozporządzenia oraz Instrukcji.

§ 46

Wszystkie rejestry, ewidencje, wykazy, o których mowa w Polityce objęte są nakazem zachowania w tajemnicy.

§ 47

Integralną część niniejszej Polityki stanowią następujące załączniki:
1) Załącznik nr 1 – Wzór wyznaczania Administratora Bezpieczeństwa Informacji w ZGKiKM;
2) Załącznik nr 2 – Wzór wyznaczania Administratora Systemu Informatycznego w ZGKiKM;
3) Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych;
4) Załącznik nr 4 – Wzór oświadczenia o zachowanie poufności;
5) Załącznik nr 5 – Wzór Wykazu zbiorów danych osobowych przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego
6) Załącznik nr 6 – Wzór rejestru stwierdzonych naruszeń;
7) Załącznik nr 7 – Wniosek o nadanie uprawnień w systemie informatycznym
8) Załącznik nr 8 – Podstawowe zasady bezpieczeństwa

Załącznik nr 1 do Polityki Bezpieczeństwa Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

WZÓR

Wrocław, dnia..... r.

Zarząd Geodezji,
Kartografii i Katastru Miejskiego we Wrocławiu

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922, z późn. zm.) oraz § 8 ust. 2 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr 13/2017 Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu z dnia 29.03.2017 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Zarządzie Geodezji Kartografii i Katastru Miejskiego we Wrocławiu, wyznaczam

Panią/Pana.....
(imię i nazwisko)
.....
(stanowisko, komórka organizacyjna)

na

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI W ZARZĄDZIE GEODEZJI, KARTOGRAFII I KATASTRU MIEJSKIEGO WE WROCŁAWIU

Administrator Bezpieczeństwa Informacji zobowiązany jest do wdrażania i nadzoru nad prawidłową realizacją czynności dotyczących przetwarzania danych osobowych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu poprzez zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, zgodnie z § 26 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr 13/2017 Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu z dnia 29.03.2017 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu.

.....
(podpis i pieczęć Administratora Danych

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz sposobów ich zabezpieczania w okresie trwania stosunku pracy, jak i po jego ustaniu.

Przyjmuję do realizacji
powierzone mi obowiązki i uprawnienia

.....
(data i podpis upoważnionego)

00000018

Załącznik nr 2 do Polityki Bezpieczeństwa Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

WZÓR

Wrocław, dnia..... r.

Zarząd Geodezji,
Kartografii i Katastru Miejskiego we Wrocławiu

Na podstawie § 8 ust. 3 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr 13/2017 Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu z dnia 29.03.2017 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu, wyznaczam

Panią/Pana.....
(imię i nazwisko, stanowisko)

na

ADMINISTRATORA SYSTEMU INFORMATYCZNEGO W ZARZĄDZIE GEODEZJI, KARTOGRAFII I KATASTRU MIEJSKIEGO WE WROCŁAWIU

Administrator Systemu Informatycznego zobowiązany jest do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w systemach informatycznych Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu oraz realizacji zadań określonych w § 27 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr 13/2017 Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu z dnia 29.03.2017 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu.

.....
(podpis i pieczęć Administratora Danych

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zobowiązuje się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz sposobów ich zabezpieczania w okresie wykonywania obowiązków związanych z przetwarzaniem danych, zmiany, odwołania a także po ustaniu stosunku pracy.

Przyjmuję do realizacji
powierzone mi obowiązki i uprawnienia

.....
(data i podpis upoważnionego)

Załącznik nr 3 do Polityki Bezpieczeństwa Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

WZÓR

Wrocław, dnia..... r.

Zarząd Geodezji,
Kartografii i Katastru Miejskiego we Wrocławiu

UPOWAŻNIENIE NR...

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922, z późn. zm.) oraz § 33 ust. 3 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do zarządzenia nr 13/2017 Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu z dnia .29.03.2017 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Panią/Pana.....
(imię i nazwisko)
.....
(stanowisko, komórka organizacyjna)

Do przetwarzania danych osobowych gromadzonych w aktach osobowych oraz w innych zbiorach, przetwarzanych przez Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu.

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ustania Pani/Pana stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

.....
(podpis i pieczęć Administratora Danych

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych oraz sposobów ich zabezpieczania w okresie trwania stosunku pracy, jak i po jego ustaniu.

Przyjmuję do realizacji
powierzone mi obowiązki i uprawnienia

.....
(data i podpis upoważnionego)

00000090

Załącznik nr 4 do Polityki Bezpieczeństwa Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

WZÓR

_____
Imię i Nazwisko

_____
Stanowisko

_____
Nazwa komórki organizacyjnej

Oświadczenie o poufności

Ja, niżej podpisana/y, oświadczam, że **zobowiązuję** się do:

1. Zachowania w tajemnicy danych osobowych, w tym sposobów ich zabezpieczenia w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu, w okresie trwania stosunku pracy, jak i po jego ustaniu,

2. Przestrzegania zasad zabezpieczania i ochrony danych osobowych przetwarzanych przeze mnie w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu, w tym do ochrony danych osobowych przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,

3. Przetwarzania danych osobowych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu wyłącznie w zakresie wskazanym w udzielonym mi upoważnieniu do przetwarzania danych,

4. Zgłaszania bezpośredniemu przełożonemu i Administratorowi Bezpieczeństwa Informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu wszelkich faktycznych prób lub podejrzeń naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych lub każdej innej formie.

Jednocześnie **oświadczam**, że zapoznałam/em się z treścią obowiązujących przepisów prawa w zakresie przetwarzania oraz ochrony danych osobowych, w szczególności z postanowieniami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922, z późn. zm.) i zasadami bezpieczeństwa przetwarzania danych osobowych określonych w Zarządzeniu nr 13/2017 Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu z dnia29.03.2017 r. w sprawie ustalenia zasad bezpieczeństwa informacji w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu i zobowiązuję się do ich przestrzegania.

Oświadczam, że znana jest mi odpowiedzialność za naruszenie podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej oraz mam świadomość, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów określonych w ustawie o ochronie danych osobowych oraz stanowi naruszenie obowiązków pracowniczych.

.....
podpis pracownika

.....
miejscowość i data

Załącznik nr 5 do Polityki Bezpieczeństwa
Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Wzór zbiorów danych osobowych przetwarzanych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Nr zbioru	Nazwa zbioru danych	Administrator Danych Osobowych Adres siedziby REGON	Przedstawiciel, o którym mowa w art. 31a ustawy	Podmiot któremu powierzono przetwarzanie danych w trybie art. 31 ustawy	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Cel przetwarzania danych w zbiorze	Kategoria osób, których dane są przetwarzane w zbiorze	Zakres danych przetwarzanych w zbiorze;	Sposób zbierania / udostępniania danych do zbioru	Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego
1.											
2.											
3.											
4.											
5.											
6.											
7.											

00000021

Załącznik nr 6 do Polityki Bezpieczeństwa
Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

0000022

Rejestr stwierdzonych naruszeń w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Lp.	Rodzaj stwierdzonego naruszenia	Rodzaj podjętych czynności	Data zgłoszenia naruszenia	Podpis osoby zgłaszającej	Podpis ABI /ASI	Podpis Administratora Danych
1.						
2.						
3.						
4.						
5.						

Załącznik nr 7 do Polityki Bezpieczeństwa Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Wrocław, dnia .....

WNIOSEK O NADANIE UPRAWNIEŃ

W SYSTEMIE INFORMATYCZNYM

Rodzaj zmiany w systemie informatycznym*:

- ☐ Nowy użytkownik
- ☐ Odebranie uprawnień w systemie
- ☐ Modyfikacja uprawnień

Imię i nazwisko użytkownika:	Komórka organizacyjna:	
Czy użytkownik posiada upoważnienie do przetwarzania danych osobowych*:	☐ Tak	☐ Nie
Opis zakresu uprawnień użytkownika w systemie informatycznym: *(nazwa aplikacji (bazy danych), w której przetwarzane są dane osobowe)*		
Podpis bezpośredniego przełożonego:	Akceptacja Dyrektora DS:	
ASI/LASI:	/:	

*Właściwe zaznaczyć

Załącznik nr 8 do Polityki Bezpieczeństwa
Zarządu Geodezji, Kartografii i Katastru
Miejskiego we Wrocławiu

Podstawowe zasady bezpieczeństwa

Zasada wiedzy koniecznej – ograniczenie dostępu do informacji jedynie do tych, które są niezbędne do wykonywania obowiązków na danym stanowisku.

Zasada odpowiedzialności za zasoby – pracownik jest odpowiedzialny za przetwarzane / powierzone mu informacje i zobowiązany jest przestrzegać ustanowionych procedur bezpieczeństwa informacji.

Zasada zamkniętego pomieszczenia – niepozostawianie osób postronnych samych w pomieszczeniu (pod nieobecność osoby upoważnionej), bezwzględnie zamykanie pomieszczeń na klucz przy ich opuszczaniu i nie pozostawianie kluczy w zamkach.

Zasada czystego biurka – niepozostawianie bez nadzoru dokumentów papierowych oraz nośników danych na biurku (płyt CD, DVD, pamięci flash USB, itp.)

Zasad poufności haseł i kart dostępu – zachowanie poufności i nieprzekazywanie osobom nieuprawnionym haseł i kart dostępu. W szczególności zasada ta dotyczy osobistych haseł dostępu do systemów teleinformatycznych i stref chronionych.

Zasada czystej tablicy – po zakończonym spotkaniu w pomieszczeniach ogólnodostępnych (sale konferencyjne, itp.) należy uprzątnąć wszystkie materiały oraz wyczyścić tablice.

Zasada czystego ekranu – blokowanie komputera przed każdym opuszczeniem pomieszczenia. W przypadku dłuższej nieobecności w pomieszczeniu konieczne jest wylogowanie się z systemu.

Zasada czystego pulpitu – na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty do folderów pod warunkiem, że w nazwie nie zawierają informacji, które mogą zostać w sposób niekontrolowany ujawnione np. podczas prezentacji.

Zasada czystych drukarek – zabieranie dokumentów z drukarek zaraz po ich wydrukowaniu. W szczególności zasada ta dotyczy dokumentów pozostawianych w drukarkach znajdujących się w innym pomieszczeniu.

Zasada czystego kosza – dokumenty papierowe z wyjątkiem materiałów promocyjnych powinny być niszczone w niszczarkach lub za pośrednictwem firmy zewnętrznej.

Zasada legalności oprogramowania – zabrania się samodzielnego instalowania oprogramowania, w tym w szczególności przechowywania na komputerze treści naruszających prawa autorskie oraz innych nielegalnych danych.

Zasada zgłaszania incydentów bezpieczeństwa – każdy z pracowników zobowiązany jest do zgłaszania incydentów związanych z bezpieczeństwem informacji, tj. nieuprawnionym ujawnieniem, zniszczeniem lub modyfikacja informacji.

Zasada korzystania z zasobów dopuszczonych przez ZGKiKM - informacje, których właścicielem jest ZGKiKM mogą być przetwarzane wyłącznie w środkach przetwarzania dopuszczonych do wykorzystania w ZGKiKM. W szczególności wzbrania się z korzystania w tym celu z prywatnych środków przetwarzania informacji.

Zasada korzystania z zasobów ZGKiKM do celów prywatnych – zabrania się wykorzystywania służbowego komputera do celów prywatnych

Zasada zapisywania i archiwizacji dokumentów w formie elektronicznej – wszystkie dokumenty służbowy wytwarzane na zasobach sieciowych ZGKiKM stanowią własność ZGKiKM. Pracownicy mają obowiązek zapisywania ich na dyskach sieciowych. Zabrania się zapisywania dokumentów służbowych na dyskach lokalnych komputerów.

Załącznik nr 2
do Zarządzenia nr 13/2017 z dnia 29.03.2017 r.
Dyrektora Zarządu Geodezji, Kartografii
i Katastru Miejskiego we Wrocławiu

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
Rozdział 1.
POSTANOWIENIA OGÓLNE

§1

Określenia i skróty użyte w Polityce bezpieczeństwa oznaczają:

1) **Administrator Systemów Informatycznych** – Z-ca Dyrektora ds. Systemów informatycznych, zwany dalej Administratorem;

2) **ASI** - Administratorzy Systemów Informatycznych – pracownicy wyznaczeni przez Administratora Danych (AD) odpowiedzialni za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązani do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych;

3) **LASI** - Lokalni Administratorzy Systemów Informatycznych – osoby wyznaczone przez Administratora Danych (AD), odpowiedzialne za wdrożenie i stosowanie zasad bezpieczeństwa danych w zakresie technicznych zabezpieczeń systemów informatycznych w pionach;

4) **Użytkownik systemu** – osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu;

5) **Przełożony użytkownika, zwany dalej przełożonym**– Z-ca Dyrektora, Kierownik Działu, Kierownik Biura - osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników;

6) **Hasło** – ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

7) **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych specjalnych identyfikatorów, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;

8) **Sieć LAN/WAN** – sieć lokalna/rozległa umożliwiająca połączenie systemów informatycznych ZGKiKM przy wykorzystaniu specjalistycznych dedykowanych urządzeń i sieci telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016 r., poz. 1489, z późn. zm.);

9) **Dane sensytywne** - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym;

10) **Rejestr udostępnionych danych osobowych, zwany dalej Rejestrem** – rejestr, w którym odnotowywane są informacje o odbiorcach danych z systemu/aplikacji, prowadzony dla danego systemu/aplikacji;

Rozdział 2
PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCHI REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMI INFORMATYCZNYMORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

§ 2

1. Osobami odpowiedzialnymi za administrację systemem informatycznym są pracownicy Biura Informatyki zwani dalej ASI/LASI.
2. ASI/LASI prowadzi ewidencję osób upoważnionych do przetwarzania danych.
3. ASI/LASI udziela użytkownikowi upoważnienia oraz ustala poziom zabezpieczeń do przetwarzania danych osobowych wg ustalonego wzoru dokumentu. Upoważnienie to przekazywane jest ASI/LASI w celu zarejestrowania go w systemie informatycznym i nadania użytkownikowi odpowiednich uprawnień w systemie. Dokument upoważnienia podlega rejestracji oraz archiwizacji.

§ 3

Dostęp do sieci informatycznej, systemów informatycznych i programów zabezpieczony jest systemem użytkowników i haseł oraz ograniczeniem dostępu do zasobów sieci. Identyfikator i hasło jednoznacznie identyfikują, weryfikują i autoryzują tożsamość użytkownika.

§ 4

1. Użytkownikom nadawane są uprawnienia do systemu informatycznego. Przyznanie, zmiana lub ograniczenie uprawnień następuje na pisemny wniosek przełożonego użytkownika złożony Administratorowi Systemów Informatycznych i jest realizowane przez ASI/LASI.
2. Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania danych obliguje Administratora Systemów Informatycznych w porozumieniu z ASI/LASI do odebrania temu użytkownikowi dostępu do systemu informatycznego, jaki dotychczas posiadał.
3. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie jest usuwany z systemu informatycznego i nie jest przydzielany innej osobie.

§ 5

Administrator Systemów Informatycznych jest zobowiązany do posiadania wykazu identyfikatorów przyznanych użytkownikom w poszczególnych systemach informatycznych powiązanych z imiennym wskazaniem użytkownika. Wykaz musi uwzględniać również użytkowników, którym odebrano uprawnienia i wyrejestrowano z systemu.

Rozdział 3
STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANEZ ICH ZARZĄDZANIEM I UŻYTKOWANIEM

§ 6

1. Użytkownik jest w pełnym zakresie odpowiedzialny za swoje hasło, w szczególności za jego okresowe zmienianie i utrzymanie w tajemnicy.
2. Użytkownik jest w pełnym zakresie odpowiedzialny za dostosowanie hasła do opisanych niżej obowiązujących reguł, jeśli przestrzegania tych reguł nie wymusza w sposób automatyczny system informatyczny lub oprogramowanie.

§ 7

Administrator Systemów Informatycznych oraz ASI/LASI musi mieć możliwość bezwarunkowej zmiany hasła użytkownika.

§ 8

1. Hasło użytkownika nie może zawierać konta ani pełnej nazwy.
2. Hasło dostępu do sieci LAN/WAN musi składać się z co najmniej 8 znaków, wskazane jest, by zawierało wielkie i małe litery, cyfry i znaki specjalne.
3. Hasło użytkownika musi być zmieniane nie rzadziej niż co 30 dni. Hasło użytkownika musi być zmienione niezwłocznie w przypadku jego ujawnienia lub podejrzenia ujawnienia.
4. Użytkownik jest zobowiązany do utrzymania swoich haseł w tajemnicy, również po utracie ich ważności.
5. Hasło przy wpisywaniu nie może być w sposób jawny wyświetlane na ekranie.
6. W przypadku nagłej potrzeby zmiany hasła do sieci LAN/WAN użytkownik powinien zgłosić się do ASI/LASI wraz z dokumentem stwierdzającym tożsamość.
7. W ZGKiKM, stosuje się poziom bezpieczeństwa przetwarzania danych adekwatnie do klasyfikacji tych danych w systemach i aplikacjach. W związku z powyższym, obowiązujące są trzy poziomy bezpieczeństwa:
1) poziom podstawowy - dla systemów i aplikacji, w których nie są przetwarzane dane osobowe sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu lub aplikacji musi się składać z co najmniej 8-iu znaków;
2) poziom podwyższony - dla systemów i aplikacji, w których są przetwarzane dane sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu i aplikacji musi składać się z co najmniej 8 znaków, i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
3) poziom wysoki - dla systemów i aplikacji, w których są przetwarzane dane sensytywne oraz co najmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych jest połączone z siecią publiczną. Wówczas należy stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania.

§ 9

1. ASI/LASI tworzy hasło jednorazowe dla użytkownika w celu pierwszego logowania do systemu. Użytkownik po zalogowaniu jest zobowiązany do natychmiastowej zmiany hasła zgodnie z przyjętymi wyżej regułami.
2. Hasła ASI/LASI przechowywane są w programowym magazynie haseł, do którego dostęp jest zabezpieczony hasłem przechowywanym jawnie w zabezpieczonej kopercie w sejfie. Dostęp do sejfu posiada Administratora Systemów Informatycznych oraz ASI/LASI.

Rozdział 4
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIAPRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 10

1. ASI/LASI monitoruje rozpoczęcie i zawieszenie pracy systemy informatycznego.
2. ASI/LASI ma prawo do monitorowania pracy urządzeń przyłączonych do sieci informatycznej pod kątem przesyłania danych i przetwarzania danych, rejestracji zdarzeń związanych z przesyłaniem i przetwarzaniem danych w oprogramowaniu oraz prawidłowości wykorzystania powierzonego użytkownikom sprzętu i oprogramowania.

§ 11

Przed rozpoczęciem pracy w sieci informatycznej użytkownik musi się w niej autoryzować przez podanie swojego identyfikatora i hasła. Dopiero po pomyślnej autoryzacji w sieci informatycznej użytkownik może uruchomić program służący do przetwarzania danych, dokonując osobnej autoryzacji w tym programie (o ile jest to wymagane).

§ 12

Sposób wymiany i przesyłania danych w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników oraz ich działań przy wykorzystaniu sieci informatycznej i oprogramowania.

§ 13

1. Informacje pozyskane w wyniku monitorowania działań użytkowników oraz pracy urządzeń są dostępne wyłącznie Administratorowi Systemów Informatycznych oraz ASI/LASI i mogą zostać wykorzystane wyłącznie do celów służbowych, związanych z bezpieczeństwem przetwarzania danych w systemach informatycznych.
2. Kontrola przetwarzania danych prowadzona jest na bieżąco przez użytkownika na każdym stanowisku merytorycznym. Nadzór prowadzi bezpośredni przełożony oraz ASI/LASI.

§ 14

W przypadku konieczności czasowego opuszczenia stanowiska pracy przyłączonego do sieci informatycznej lub służącego do przetwarzania danych wiążącego się ze stratą pola widzenia swojego stanowiska, użytkownik powinien:
1) wylogować się z programu lub sieci informatycznej;
2) zablokować stację roboczą, tak aby odblokowanie wymuszało podanie hasła.

§ 15

1. Użytkownik jest zobowiązany do uniemożliwienia odczytania informacji z monitora przez osoby nieuprawnione.
2. Użytkownik jest zobowiązany do wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji roboczej.

§ 16

W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu, użytkownik jest zobowiązany do bezzwłocznego powiadomienia o tym fakcie ASI/LASI.

§ 17

W pomieszczeniu, w którym ustawiony jest serwer, może pracować tylko ASI/LASI i osoba przez niego upoważniona. Przebywanie w tym pomieszczeniu osób nieupoważnionych do przetwarzania danych możliwe jest pod nadzorem ASI/LASI.

Rozdział 5
PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH

§ 18

1. Kopią zapasową objęte są dane znajdujące się na serwerach sieci informatycznej.
2. Za sporządzenie i bezpieczeństwo kopii zapasowych odpowiedzialny jest ASI/LASI.
3. Kopia zapasowa wykonywana jest przez kopiowanie całości danych.
4. Harmonogram sporządzania kopii zapasowych musi gwarantować dostępność w każdej chwili trzech kopii: z ostatniego dnia, z końca ubiegłego tygodnia oraz z końca ubiegłego półrocza.

§ 19

Z uwagi na różnorodność danych podlegających zabezpieczaniu dla każdego systemu bądź rodzaju danych ustala się odrębny harmonogram wraz z metodą tworzenia kopii, uwzględniający postanowienia niniejszego punktu.

§ 20

W systemach informatycznych, które opierają się o pracę w technologii klient-serwer, kopie bezpieczeństwa wykonuje się po stronie serwera.

§ 21

Użytkownicy we własnym zakresie odpowiadają za sporządzenie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych, przy jednoczesnym obowiązku dopilnowania, aby dane na lokalnym dysku twardym nie zawierały danych osobowych.

§ 22

Po wykonaniu kopii zapasowej ASI/LASI ma obowiązek wykonania weryfikacji poprawności wykonanej kopii.

Rozdział 6
SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA KOPII ZAPASOWYCH

§ 23

1. Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich osobom nieupoważnionym.
2. Niedopuszczalne jest przechowywanie danych oraz ich kopii wyłącznie na jednym urządzeniu. W związku z tym wykonuje się kopie na nośnikach zewnętrznych.
3. Kopie zapasowe przechowuje się w sejfie umieszczonym w zarządzie ZGKiKM oraz w skrytce bankowej. Dostęp do kopii posiada ASI/LASI. Potwierdzenie wykonania i złożenia kopii jest odnotowywane w Książce Ewidencji Baz Danych.
4. Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
5. Nośniki jednorazowe zawierające nieaktualne kopie danych likwiduje się. Likwidacja polega na ich fizycznym zniszczeniu w taki sposób, aby nie można było odczytać ich zawartości.
6. Nośniki wielorazowego użytku wykorzystuje się ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
7. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.
8. Za zniszczenie zbędnych wydruków i innych zbędnych dokumentów zawierających dane osobowe odpowiedzialny jest Kierownik komórki organizacyjnej.
9. Za skasowanie zbędnych danych, zniszczenie zbędnych danych lub zniszczenie zbędnych nośników odpowiedzialny jest ASI/LASI.
10. Kopie zapasowe przechowuje się przez okres:
1) dzienne przez 21 dni;
2) tygodniowe minimum ostatnie 2 tygodnie;
3) półroczne przez czas nieograniczony.

Rozdział 7
SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, CELEM KTÓREGO JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO LUB INNE INGERENCJE W TEN SYSTEM

§ 24

System informatyczny jest zabezpieczany przez zastosowanie rozwiązań sprzętowych i programowych.

§ 25

1. Za aktualność stosowanych zabezpieczeń, dostosowywanie do aktualnych potrzeb, konfigurację i zarządzanie nimi odpowiada ASI/LASI.
2. ASI/LASI ma obowiązek zgłaszać na piśmie Administratorowi Systemów Informatycznych wszelkie potrzeby lub zauważone niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.
3. Wykorzystywane rozwiązania muszą zapewnić automatyczne działania w przypadku wykrycia zagrożenia w systemie informatycznym oraz zapewnić możliwość konfiguracji odpowiednio do potrzeb.

§ 26

W przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są zobowiązani bezzwłocznie powiadomić o tym fakcie ASI/LASI, który po usunięciu zagrożenia sprawdza system i przywraca go do pełnej funkcjonalności.

§ 27

Dla minimalizacji zagrożeń należy dążyć do maksymalnej unifikacji sprzętu działającego w systemie informatycznym, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych.

§ 28

1. Bezwzględnie zakazuje się użytkownikom samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji. Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody ASI/LASI, po uprzednim sprawdzeniu nośnika informacji przez ASI/LASI pod względem bezpieczeństwa dla systemu informatycznego.
2. Bezwzględnie zakazuje się użytkownikom wykorzystywania powierzonego im sprzętu informatycznego, oprogramowania i dostępu do zasobów informatycznych do jakichkolwiek celów innych niż wykonywanie powierzonych im obowiązków służbowych lub związanych z własną edukacją i dokształcaniem.
3. Bezwzględnie zakazuje się użytkownikom samowolnego instalowania na stacjach roboczych jakiegokolwiek oprogramowania z jakiegokolwiek źródła, za wyjątkiem aktualizowanych automatycznie komponentów systemu operacyjnego.

§ 29

W przypadku konieczności zainstalowania innego oprogramowania niż to, które otrzymuje do dyspozycji na powierzonej mu stacji roboczej, użytkownik zgłasza taką potrzebę swojemu bezpośredniemu przełożonemu, a ten wnioskuje pisemnie potrzebę wraz z uzasadnieniem Administratorowi Systemów Informatycznych. Administrator Systemów Informatycznych w porozumieniu z ASI/LASI decyduje o faktycznym zaistnieniu takiej konieczności. W

przypadku pozytywnej opinii jedyną osobą uprawnioną do zainstalowania dodatkowego oprogramowania jest ASI/LASI.

§ 30

Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić ASI/LASI.

§ 31

Użytkownicy są bezpośrednio odpowiedzialni za zainstalowane na powierzonych im stacjach roboczych oprogramowanie oraz mają obowiązek zgłaszać wszelkie wątpliwości w tym zakresie ASI/LASI, ze szczególnym uwzględnieniem zmian, które zostały wprowadzone podczas ich nieobecności.

Rozdział 8
PROCEDURY WYKONANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

§ 32

1. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych oraz nośników informacji dokonuje stosownie do potrzeb ASI/LASI.
2. W przypadku przekazywania stacji roboczej do naprawy należy zdemontować nośniki informacji.

§ 33

Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności niezwiązanych bezpośrednio z jego eksploatacją lub niedopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.

§ 34

Użytkownik ma obowiązek niezwłocznie powiadomić ASI/LASI o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do naruszenia lub próby naruszenia bezpieczeństwa danych.

§ 35

W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji ASI/LASI zobowiązany jest:
1. przetestować system informatyczny do przetwarzania danych w celu ustalenia przyczyny utraty informacji
2. odtworzyć, przy uwzględnieniu nakładu pracy:
1) część danych – ręcznie;
2) całość danych przy użyciu kopii zapasowej.

Rozdział 9
PROCEDURY POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH

§ 36

1. Naruszeniem zabezpieczenia danych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub ich usunięcia, a w szczególności:
1) nieautoryzowany dostęp;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.
2. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych każdy pracownik zatrudniony przy przetwarzaniu danych jest zobowiązany przerwać przetwarzanie danych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, Administratorowi Bezpieczeństwa Informacji, ASI/LASI lub Administratorowi Systemów Informatycznych, a następnie postępować stosownie do podjętej przez niego decyzji.
3. Zgłoszenie naruszenia zabezpieczeń danych powinno zawierać:
1) opisanie symptomów naruszenia zabezpieczeń danych;
2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie zabezpieczeń danych;
3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 37

Administrator Bezpieczeństwa Informacji podejmuje wszelkie działania mające na celu:
1) minimalizację negatywnych skutków zdarzenia;
2) wyjaśnienie okoliczności zdarzenia;
3) zabezpieczenie dowodów zdarzenia;
4) umożliwienie dalszego bezpiecznego przetwarzania danych.

§ 38

Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
1) żądania wyjaśnień od pracowników;
2) korzystania z pomocy konsultantów;
3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych.

ROZDZIAŁ 10
POSTANOWIENIA KOŃCOWE

§ 30

W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują:
1. Norma PN-I-13335-1 „Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych".
2. Norma PN-ISO/IEC-17799 „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.

3. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2016 r., poz. 922, z późn. zm.).
4. 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).

Integralną część niniejszej Instrukcji zarządzania systemem informatycznym stanowią następujące załączniki:

1) Załącznik nr 1 - Regulamin korzystania z Sieci LAN/WAN przez pracowników ZGKiKM;
2) Załącznik nr 2 – Regulamin korzystania z poczty elektronicznej przez pracowników ZGKiKM;
3) Załącznik nr 3 - Regulamin korzystania z usługi IP VPN;
4) Załącznik nr 4 - Zasady użytkowania sprzętu komputerowego przez pracowników ZGKiKM;
5) Załącznik nr 5 - Zasady udzielania pomocy użytkownikom sprzętu komputerowego w ZGKiKM;
6) Załącznik nr 6 - Rejestr kopii zapasowych;
7) Załącznik nr 7 - Zgłoszenie naruszenia bezpieczeństwa systemu informatycznego.

Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym w Zarządzie Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Regulamin korzystania z Sieci LAN/WAN przez pracowników ZGKiKM

§ 1

Regulamin ustala zasady korzystania z sieci LAN/WAN ZGKiKM przez pracowników ZGKiKM.

§ 2

1. Sieć LAN/WAN ZGKiKM tworzą:
1) sieci lokalne poszczególnych jednostek organizacyjnych ZGKiKM oraz łącza między nimi;
2) ogólno-dostępowe serwery kont i usług sieciowych.
2. Funkcję ASI/LASI ZGKiKM pełnią osoby wyznaczone przez Administratora Danych (AD).

§ 3

1. Użytkownikiem systemu w ZGKiKM jest każda osoba korzystająca z komputera bądź terminala podłączonego do sieci LAN/WAN ZGKiKM.
2. Konto użytkownika systemu to zarejestrowane uprawnienie do pracy na jednym z serwerów w sieci LAN/WAN ZGKiKM.
3. Konta na serwerze są przydzielane wszystkim pracownikom ZGKiKM zgodnie z ustaloną procedurą:
1) Przełożony użytkownika zgłasza potrzebę założenia konta dla nowego pracownika zgodnie z wnioskiem stanowiącym załącznik nr 9do Polityki bezpieczeństwa przy posługiwaniu się systemem informatycznym w przetwarzaniu danych w Zarządzie Geodezji, Kartografii i Katastru Miejskiego;
2) Użytkownik systemu może mieć tylko jedno konto na serwerze. Uprawnienia do posiadania kont są kontrolowane na podstawie danych przekazywanych przez Zastępcę Dyrektora, Kierownika Biura, Kierownika Działu, osobę przełożoną do Administratora Systemów Informatycznych;
3) Konto użytkownika systemu daje uprawnienia do korzystania z poczty elektronicznej i innych usług sieciowych ZGKiKM wymagających uwierzytelnienia. W uzasadnionych przypadkach na wniosek przełożonego użytkownika, ASI/LASI mogą zmienić uprawnienia konta;
4) ASI/LASI określa warunki techniczne korzystania z kont oraz ograniczenia rozmiaru zużywanej przestrzeni dyskowej;
5) Pracownicy ZGKiKM korzystają z poczty poprzez wskazanego przez ASI/LASI klienta serwera pocztowego lub dowolną przeglądarkę internetową;
6) Pojemność skrzynek pocztowych pracowników ZGKiKM jest ograniczona – limit 2GB. Po przekroczeniu tej wartości zostanie zablokowana możliwość wysyłania wiadomości do momentu oczyszczenia skrzynki pocztowej. W uzasadnionych przypadkach na wniosek przełożonego użytkownika, ASI/LASI może zwiększyć wielkość skrzynki;
7) Pracownicy mają możliwość przechowywania swojej poczty na stacjach roboczych, wiąże się to jednak z tym, że pełna odpowiedzialność za ewentualną utratę danych jest po stronie użytkownika systemu;

8) Dział Kadr przekazuje dane dotyczące rozwiązania/zawarcia umowy o pracę z pracownikami ZGKiKM do Administratora Systemów Informatycznych;
9) W przypadku pracownika, z którym został rozwiązany stosunek pracy, ASI/LASI zobowiązany jest zarchiwizować dane tego użytkownika systemu a następnie na polecenie Administratora Systemów Informatycznych skasować konto z uprawnieniami w systemie i aplikacji;
10) Konta pracowników, którzy pozostają w stosunku pracy, ale utracili uprawnienia do ich posiadania są kasowane po upływie 2 miesięcy;

§ 4

1. Każdy użytkownik systemu ZGKiKM powinien postępować zgodnie z powierzonymi mu obowiązkami, a w szczególności z poniższymi zasadami:
1) używanie poczty elektronicznej tylko do celów służbowych;
2) korzystanie z Internetu tylko do celów służbowych;
3) korzystanie z systemów i aplikacji ZGKiKM tylko do celów służbowych;
2. Zabronione jest:
1) wysyłanie masowej poczty kierowanej do losowych odbiorców (spam);
2) udostępnianie treści chronionych prawem autorskim (filmy, czy utwory muzyczne);
3) udostępnianie treści zakazanych (np. pornografia);
4) nieuzasadnione wynoszenie danych zawartych na nośnikach poza ZGKiKM.
3. Pracodawca zastrzega sobie prawo do monitorowania ruchu w sieci LAN/WAN ZGKiKM, w zakresie określonym w powyższych ust. 1 i 2.
1) Jeżeli zaistnieje potrzeba podłączenia komputera prywatnego (laptop) pracownika do sieci LAN/WAN ZGKiKM, wymaga to następujących czynności;
2) akceptacji przełożonego pracownika, akceptacji Administratora Systemów Informatycznych.
4. Zabrania się podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci.
5. Zabrania się uruchamiania aplikacji, które mogą zakłócić i destabilizować pracę systemu lub sieci komputerowej, bądź naruszyć prywatność zasobów systemowych.
6. W przypadku naruszenia zasad opisanych w ust. 1 właściwy ASI/LASI blokuje dostęp do konta użytkownika. O tym fakcie powiadamiany jest Administrator Systemów Informatycznych i przełożony pracownika.
7. W przypadku stwierdzenia, że komputer dołączony do sieci LAN/WAN generuje strumień danych zakłócający pracę sieci lub wskazujący na używanie tego komputera, jako niezarejestrowanego serwera danych, ASI/LASI ma prawo zablokować dostęp do tego komputera do czasu wyjaśnienia sprawy. O tym fakcie powiadamiany jest Administrator Systemów Informatycznych i przełożony pracownika.

Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym w Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Regulamin korzystania z poczty elektronicznej przez pracowników ZGKiKM

§ 1

Każdy pracownik zatrudniony w ZGKiKM otrzymuje dostęp do elektronicznej skrzynki pocztowej.

§ 2

Adres konta pocztowego tworzony jest na podstawie wzorca:nazwisko1literaimienia@zgkikm.wroc.pl

§ 3

Pracownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie do korespondencji służbowej, związanej z działalnością ZGKiKM.

§ 4

Przy korespondencji pracownik zobowiązany jest do stosowania następujących reguł:
1) sprawdzać skrzynkę pocztową przynajmniej raz dziennie;
2) bezzwłocznie odpowiadać na każdy list;
3) odpowiadając na list, zawsze określać jego temat;
4) umieszczać swój podpis.

§ 5

Zabrania się przesyłania na prywatne skrzynki mailowe jakichkolwiek dokumentów związanych z działalnością ZGKiKM.
Wykorzystywanie w czasie pracy poczty elektronicznej do prywatnych celów można stanowić podstawę wyciągnięcia konsekwencji służbowych przewidzianych prawem.

§ 6

E-maile wysłane z firmowej skrzynki pocztowej stanowią własność pracodawcy i pracodawca może je nadzorować.

§7

Z uwagi na konieczność zapewnienia ochrony interesu i bezpieczeństwa pracodawca zastrzega sobie prawo do wglądu we wszystkie wiadomości pracownika o charakterze służbowych (zarówno w skrzynce odbiorczej, w wiadomościach wysłanych jak i innych folderach)

§ 8

Wgląd do służbowej korespondencji pracowników oraz ich poczty elektronicznej może nastąpić po wcześniejszym uprzedzeniu pracownika.
Pracodawca ma prawo weryfikacji przestrzegania przez pracownika zasad korzystania ze służbowej poczty elektronicznej określonej w Regulaminie.

00000038

Załącznik nr 3 do Instrukcji zarządzania systemem informatycznym w Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Regulamin korzystania z usługi IP VPN
w ramach infrastruktury IT będącej własnością ZGKiKM

§ 1
Cel regulaminu

Celem niniejszego regulaminu jest wskazanie zasad oraz reguł korzystania z zdalnego dostępu do sieci komputerowej poprzez połączenia Virtual Private Network (VPN) w technologii L2TP oraz IPSec.

§ 2
Zakres regulaminu

Niniejszy regulamin dotyczy wszystkich pracowników ZGKiKM, współpracowników, podwykonawców, konsultantów, pracowników czasowych oraz innych pracowników firm trzecich korzystających z zasobów wewnętrznych korzystających z połączeń VPN, zwanych dalej użytkownikami.

§ 3
Polityka dostępu

1. Autoryzowani Użytkownicy mogą korzystać z usługi sieci VPN, która to jest usługą zarządzaną na bazie autoryzacji. Polityka dostępu do sieci VPN stanowi, iż użytkownicy są odpowiedzialni za bezpieczeństwo korzystania z usługi, w szczególności za zachowanie zasad opisanych w ust. 2 poniżej.
2. Obowiązkiem każdego Użytkownika korzystającego z sieci VPN i co za tym idzie zasobów sieciowych jest bezwzględne przestrzeganie reguł opisanych poniżej:

1) Obowiązkiem każdego Użytkownika, który posiada dostęp do sieci VPN jest dopilnowanie tego, iż żaden inny nieautoryzowany podmiot/użytkownik nie będzie korzystał z praw przydzielonych Użytkownikowi;
2) Dostęp do sieci VPN będzie następował poprzez wykorzystanie konta domenowego lub imiennego certyfikatu oraz silnego hasła do certyfikatu lub loginu do konta oraz hasła do konta;
3) Obowiązkiem Użytkownika jest wykorzystanie haseł zgodnych z obowiązującą w ZGKiKM polityką bezpieczeństwa w przypadku wykorzystania konta domenowego lub tzw. „silnych haseł" dla zwykłych kont składających się minimalnie z:
   a) Co najmniej 13 znaków alfanumerycznych;
   b) Co najmniej 2 cyfr;
   c) Co najmniej 3 znaków specjalnych takich jak „!@#$%^&*()_+=-|";
   d) Co najmniej 2 dużych liter.
4) Użytkownik w żadnym wypadku nie może:
   a) Przechowywać certyfikatu w/na komputerze, w miejscach publicznych takich jak kafejki internetowe, komputery w hotelu, etc.;
   b) Przechowywać certyfikatu w usługach online takich jak np. dropbox, mesh, etc.;
   c) Przechowywać hasła oraz loginu w postaci niezaszyfrowanej np. w pliku tekstowym, na kartce, etc..
5) Komputer połączony poprzez sieć VPN musi posiadać system antywirusowy z uaktualnionymi definicjami bazy wirusów, przy czym system antywirusowy musi być podczas całego połączenia włączony;

6) Podwójne szyfrowanie za wyjątkiem usług RDP oraz usług SSH do serwerów jest zabronione;
7) Korzystanie z zasobów sieci Internet poprzez sieć VPN jest zabronione;
8) Korzystanie z połączeń, adresów, lokalizacji i technologii nie zaaprobowanych przez zespół operacyjny sieci firmowej jest zabronione;
9) Użytkownicy korzystający z prywatnych urządzeń dostępowych (o ile uzyskali zgodę na wykorzystanie tych urządzeń do celów służbowych) takich jak komputery, laptopy, palmtopy, tablety, itp. w czasie połączenia z siecią VPN również podlegają niniejszym zapisom regulaminu i takim samym regułom jakie obowiązują w sieci;
10) Użytkownicy korzystający z sieci VPN są limitowani maksymalnie do 24 godzinnego połączenia ciągłego, a w wypadku wykrycia nieaktywności połączenie zostanie automatycznie rozłączone po 20 minutach;
11) Osoby trzecie korzystające z sieci VPN są limitowane maksymalnie do 8 godzinnego połączenie ciągłego, a w wypadku wykrycia nieaktywności połączenie zostanie automatycznie rozłączone po 20 minutach;
12) Użytkownicy są zobowiązani do nie łączenia się z siecią w przypadku, gdy takie połączenie nie jest uzasadnione np. zleconą pracą, delegowanym zadaniem, obowiązkiem stałym w wypadku choroby lub delegacji ew. innej logicznie i formalnie usprawiedliwionej nieobecności;
13) Obowiązkiem każdego Użytkownika sieci VPN jest upewnienie się, iż w tym samym czasie urządzenie nie jest podpięte do innej sieci w szczególności sieci typu p2p (peer to peer) oraz m2m (mail to mail);
14) Wykorzystanie sieci VPN do innych czynności niż wykonywanie zadań służbowych (np. przeglądanie sieci Internet, pobieranie plików) jest zabronione.
3. Użytkownik korzystający z połączenia VPN zgadza się na:
1) Monitorowanie zachowania użytkownika w sieci włączając w to takie elementy jak: poczta, dostęp do zasobów plikowych, dostęp do zasobów teleinformatycznych np. sesje SSH, sesje RDP, itp.;
2) Przeszkolenie z zasad prawidłowego korzystania z sieci VPN;
3) Cykliczną zmianę hasła do konta dostępowego, nie rzadziej niż co 90 dni.

§ 4

Naruszenie regulaminu

Każdy Użytkownik akceptujący i podpisujący niniejszy dokument, któremu udowodni się niestosowanie do niniejszego regulaminu lub ominie jego zapisy może być pociągnięty do odpowiedzialności dyscyplinarnej włączając w to rozwiązanie umowy o współpracę/pracę, niezależnie od odpowiedzialności karnej wynikającej z obowiązujących przepisów prawa.

00000040

Załącznik nr 4 do Instrukcji zarządzania systemem informatycznym w Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Zasady użytkowania sprzętu komputerowego przez pracowników ZGKiKM.

§ 1

Zasady użytkowania sprzętu komputerowego przez pracowników ZGKiKM, zwane dalej zasadami, określają prawa i obowiązki użytkowników sprzętu komputerowego.

§ 2

Ilekroć w zasadach jest mowa o:

1. **Helpdesk** - rozumie się przez to pracowników Biura Informatyki, Biura Miejskiego Systemu Informacji oraz Działu Eksploatacji i Napraw przyjmujących i realizujących zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania komputerowego,
2. **sprzęcie komputerowym** - rozumie się przez to komputer oraz urządzenia peryferyjne, w tym: monitor, drukarka, skaner, aparat telefoniczny wymagające do swojego działania połączenia z komputerem,
3. **nośniki informatyczne** - urządzenia umożliwiające zapisywanie i przenoszenie danych (np. dyskietka, twardy dysk, płyta CD, pamięci masowe flash).

§ 3

1. Użytkownikowi systemu przysługuje prawo:

1) do korzystania ze sprzętu komputerowego i sieci LAN/WAN wyłącznie w zakresie powierzonych mu zadań,;

2) do korzystania z oprogramowania komputerowego zgodnie z umowami i ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj. Dz. U. z 2016 r., poz. 666 z późn. zm.).

§ 4

Informacje zapisane na nośnikach informatycznych należą do pracodawcy - ZGKiKM.

§ 5

O przekazaniu sprzętu komputerowego użytkownikowi decyduje przełożony użytkownika.

§ 6

Użytkownik jest materialnie odpowiedzialny za sprzęt komputerowy, który otrzymał do wykonywania obowiązków służbowych.

§ 7

Dział Eksploatacji i Konserwacji prowadzi sprawy w zakresie użytkowania sprzętu komputerowego i oprogramowania komputerowego, a w szczególności:

1. Sprawuje nadzór nad wykonaniem umów, dotyczących zakupu/serwisu sprzętu i oprogramowania,
2. Prowadzi ewidencję sprzętu i oprogramowania,
3. Zabezpiecza sprawne działanie sprzętu komputerowego i oprogramowania,
4. Zapewnia standardy sprzętu komputerowego i oprogramowania spełniające wymagania ZGKiKM.

§ 8

1. W przypadku zmiany miejsca pracy użytkownika systemu na inną komórkę organizacyjną w ZGKiKM, sprzęt komputerowy może pozostać w dotychczasowej komórce organizacyjnej.

2. Na przeniesienie sprzętu komputerowego wraz z użytkownikiem systemu do nowej komórki organizacyjnej musi wyrazić zgodę dotychczasowy przełożony użytkownika.
3. Użytkownik systemu jest zobowiązany do przekazania informacji do Działu Eksploatacji i Konserwacji o przeniesieniu pracownika wraz ze sprzętem komputerowym do nowej komórki organizacyjnej.
4. Przełożony użytkownika zobowiązany jest do:
1) zlecenia Helpdesk zmiany lokalizacji sprzętu komputerowego;
2) informowania Helpdesk o przekazaniu sprzętu innemu użytkownikowi.

§ 9

Każdy użytkownik systemu posiada identyfikator i hasło lub kartę inteligentną, które zabezpieczają dostęp do komputera, sieci LAN/WAN, baz danych i skrzynki pocztowej użytkownika.

§ 10

1. Zabronione jest:
1) podłączanie przez użytkownika własnych urządzeń do sprzętu komputerowego lub sieci LAN/WAN;
2) podłączania innych urządzeń niż informatyczne do wydzielonej sieci energetycznej do zasilania komputerów;
3) instalowania oprogramowania na sprzęcie komputerowym;
4) przemieszczenia sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany użytkownika bez uzgodnienia z Helpdesk;
5) fizyczne ingerowanie w konfigurację sprzętową urządzeń;
6) samowolne odłączanie od sieci lub włącznie do sieci LAN/WAN sprzętu komputerowego;
7) udostępnianie swojego identyfikatora i hasła do pracy innym osobom;
8) pozyskiwanie informacji z komputerów innych użytkowników bez ich wiedzy;
9) wykonywanie czynności, które mogą spowodować zakłócenia lub awarię sieci LAN/WAN;
10) wynoszenie poza miejsce pracy nośników zawierających dane oraz przesyłanie danych pocztą elektroniczną na zewnątrz.

§ 11

1. Na stanowiskach pracy, na których używany jest sprzęt komputerowy obowiązują szczegółowe zasady jego użytkowania:
1) zakaz spożywania posiłków przy sprzęcie komputerowym;
2) zapewnienie warunków umożliwiających swobodne działanie układu chłodzenia użytkowanego sprzętu komputerowego;
3) utrzymanie czystości przy stanowiskach komputerowych;
4) zapewnienie odpowiedniego miejsca na lokalizację sprzętu komputerowego;
5) odpowiednie meble;
6) ustawienie z dala od źródeł wilgoci, grzejników lub innych substancji mogących zakłócić prawidłowe działanie sprzętu komputerowego.

§ 12

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala Administratora Danych (AD) za wiedzą Administratora Bezpieczeństwa Informacji (ABI).
2. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych

informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed ich zniszczeniem, a w szczególności do:
1) transportowania komputera w bagażu podręcznym;
2) nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp.;
3) przenoszenia komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych;
4) użytkowania komputera w sposób minimalizujący ryzyko dostępu do przetwarzanych danych przez osoby nieupoważnione. Zabrania się użytkowania komputera w miejscach publicznych i w środkach transportu publicznego, dopuszczania osób nieupoważnionych do korzystania z komputera przenośnego na którym przetwarzane są dane osobowe.
3. ASI/LASI, w której zlokalizowana jest jednostka organizacyjna użytkownika komputera przenośnego zobowiązany jest do podejmowania działań mających na celu zabezpieczenie komputerów przenośnych. W szczególności powinien on:
1) dokonać konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe;
2) zabezpieczyć dyski komputerów przenośnych poprzez zastosowanie oprogramowania szyfrującego;
3) dokonać na komputerze przenośnym instalacji i konfiguracji oprogramowania antywirusowego;
4) oznaczyć komputer przenośny programowo lub fizycznie w sposób identyfikujący właściciela tego urządzenia z wskazaniem jednostki organizacyjnej i jej adresu jako właściciela komputera.
W razie zgubienia lub kradzieży sprzętu pracownik zobowiązany jest do natychmiastowego powiadomienia o tym fakcie Administratora Danych (AD), Administratora Bezpieczeństwa Informacji (ABI) oraz ASI/LASI
Użytkownik sprzętu komputerowego przenośnego zobowiązany jest do zapoznania się i stosowania warunków umowy ubezpieczenia.

Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym w Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

§ 1

Zasady udzielania pomocy użytkownikom sprzętu komputerowego w ZGKiKM, zwane dalej zasadami, określają zasady postępowania w przypadku wystąpienia problemów w użytkowaniu sprzętu komputerowego lub zainstalowanego oprogramowania

§ 2

Ilekroć w Zasadach jest mowa o:

1. **Helpdesk** - rozumie się przez to pracowników Biura Informatyki, Biura Miejskiego Systemu Informacji oraz Działu Eksploatacji i Napraw przyjmujących i realizujących zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania komputerowego,
2. **sprzęcie komputerowym** - rozumie się przez to komputer oraz urządzenia peryferyjne, w tym. monitor, drukarka, skaner, wymagające do swojego działania połączenia z komputerem,

§ 3

1. Zgłaszanie problemów z użytkowaniem sprzętu komputerowego i udzielanie pomocy użytkownikowi odbywa się w następujący sposób:
1) użytkownik zgłasza awarię do Helpdesk (systemowo, telefonicznie, mailowo, osobiście) który prowadzi rejestr zgłoszeń problemów;
2) Helpdesk rozwiązuje zgłoszony problem lub przekazuje zlecenie naprawy do realizacji odpowiedniemu specjaliście w danym biurze, dziale.
2. Pracownik Helpdesk:
1) nawiązuje kontakt z użytkownikiem;
2) dokonuje oceny problemu;
3) podejmuje działania mające na celu usunięcie zaistniałego problemu;
4) w przypadku braku możliwości usunięcia problemu ze sprzętem komputerowym, zgłasza do serwisu zewnętrznego w celu dokonania naprawy serwisowej.
3. Helpdesk informuje użytkownika o braku możliwości naprawy sprzętu we własnym zakresie oraz przekazuje sprzęt komputerowy do serwisu i przedstawia użytkownikowi możliwości udostępnienia sprzętu zastępczego na czas naprawy.

§ 4

Helpdesk sporządza miesięczną analizę interwencji oraz awaryjności sprzętu i przedstawia raport z wynikami analizy do Z-cy Dyrektora ds. Systemów Informatycznych.

§ 5

W przypadku konieczności oddania sprzętu komputerowego do zewnętrznego serwisu – pracownik Helpdesk, który ma przypisane dane zgłoszenie, wymontowuje i zabezpiecza dysk twardy oraz inne nośniki danych zainstalowane w danym sprzęcie.

§ 6

1. W przypadku konieczności przekazania dysku komputera do naprawy poza miejsce użytkowania komputera:
1) pracownik Helpdesk dokonuje zapisania danych na dysku sieciowym oraz nośniku CD lub DVD, a następnie kasuje dane użytkownika w sposób uniemożliwiający ich odczytanie, ze względu na poufność danych zapisanych na dyskach użytkownika;

2) w przypadku awarii dysku twardego i konieczności podjęcia próby odtworzenia danych, zadanie to powierzane jest specjalistycznym firmom zewnętrznym, na podstawie zawartych umów.

Załącznik nr 6 do Instrukcji zarządzania systemem informatycznym w Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

Data	Temat i liczba kopii	Rodzaj nośnika magnetycznego oraz dane identyfikacyjne urządzenia sporządzającego kopię	Data wykonania kopii	Nazwisko i imię osób składających kopię	Podpis	Uwagi

00000046

Załącznik nr 7 do Instrukcji zarządzania systemem informatycznym w Zarządu Geodezji, Kartografii i Katastru Miejskiego we Wrocławiu

ZGŁOSZENIE NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

DO:	Administrator Bezpieczeństwa Informacji				
OD:	Nazwisko i imię	Stanowisko	Komórka organizacyjna	Telefon	Podpis

Data i czas zajścia/zgłoszenia incydentu:	
Opis incydentu:	
Jakie przeciwdziałania zostały podjęte?	
Kto uczestniczył w incydencie?	
Kto został poinformowany o incydencie?	

Proszę podać również poniższe informacje:

Lokalizacja stacji roboczej/serwera	Nazwa stacji roboczej/serwera oraz adres IP	Nazwisko użytkownika stacji roboczej/ administratora serwera	Telefon użytkownika stacji roboczej/ administratora serwera	Uwagi

Informacje o sprzęcie:	Komputer	Monitor	Drukarka (podłączona bezpośrednio)	Inne
Producent				
Nrseryjny				

.....

Data i godzina przyjęcia zgłoszenia

.....

Nazwisko (czytelne) i podpis osoby Przyjmującej zgłoszenie