POWIATOWY ZAKŁAD KATASTRALNY
we Wrocławiu
ul. T. Kościuszki 131
50-440 Wrocław

Zarządzenie nr 8 /2023
-18- Dyrektora Powiatowego Zakładu Katastralnego we Wrocławiu
z dnia 7 lipca 2023 r.

w sprawie wprowadzenia polityki bezpieczeństwa informacji, w tym danych osobowych, w Powiatowym Zakładzie Katastralnym we Wrocławiu

Na podstawie § 16 pkt 1 Regulaminu organizacyjnego Powiatowego Zakładu Katastralnego we Wrocławiu stanowiącego załącznik do Uchwały Nr 155/2022 Zarządu Powiatu Wrocławskiego z dnia 24 sierpnia 2022 r. oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz.U. 2019 r. poz. 1781), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 r., poz. 2247), rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz .Urz. UE L119 z 4 maja 2016 r.) zarządzam co następuje:

§ 1

1. Wprowadzam Politykę Bezpieczeństwa Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu , stanowiącą Załącznik nr 1 do niniejszego Zarządzenia.
2. Wprowadzam System Zarządzania Bezpieczeństwem Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu, stanowiącą Załącznik nr 2 do niniejszego Zarządzenia.
3. Wprowadzam Wymagania w Zakresie Bezpieczeństwa Informacji w Systemach Informatycznych w Powiatowym Zakładzie Katastralnym we Wrocławiu, stanowiącą Załącznik nr 4 do niniejszego Zarządzenia.

§ 2

1. Zobowiązuje się pracowników Powiatowego Zakładu Katastralnego we Wrocławiu do zapoznania się z treścią niniejszego Zarządzenia i jego stosowania.
2. Zapoznanie się z niniejszym Zarządzeniem pracownik potwierdza poprzez podpisanie oświadczenia o zapoznaniu się z dokumentami, o których mowa w § 1, stanowiącego Załącznik nr 3 do niniejszego Zarządzenia.

§ 3

Wykonanie niniejszego Zarządzenia powierza się Kierownikowi Działu Ogólno-Administracyjnego.

§ 4

Traci moc Zarządzenie nr 9/2017 Dyrektora Powiatowego Zakładu Katastralnego we Wrocławiu z dnia z dnia 22 września 2017 w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Powiatowym Zakładzie Katastralnym we Wrocławiu.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Maciej Tobjasz

Załącznik Nr 1
do Zarządzenia Nr 8 /2023
Dyrektora Powiatowego Zakładu Katastralnego we Wrocławiu
z dnia 7 lipca 2023 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI w POWIATOWYM ZAKŁADZIE KATASTRALNYM we WROCŁAWIU

SPIS TREŚCI

Rozdział 1.
Postanowienia ogólne

§ 1.
Podstawy prawne

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (RODO)(Dz. Urz. UE L119 z 4 maja 2016 r.) zwane dalej Rozporządzeniem.
2. Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (t. j. Dz. U. z 2019 r. poz. 1781).
3. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (t. j. Dz. U. 2017 r. poz. 2247).

§ 2.
Słownik pojęć

1. **Active Directory (AD)** – usługa katalogowa dla systemów Windows oferująca dostęp do sieci wewnętrznej.
2. **Administrator Danych Osobowych** (**ADO**) **/ administrator danych** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem Danych Osobowych, w rozumieniu niniejszego dokumentu jest Powiatowy Zakład Katastralny we Wrocławiu reprezentowany przez Dyrektora.
3. **Audyt** – systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony informacji danych osobowych, na podstawie określonych kryteriów, wymagań polityk i procedur, dający informację o zapewnieniu lub brak zapewnienia poprawności funkcjonowania systemu bezpieczeństwa. Audyt może być przeprowadzany w celach doradczych (zadania doradcze).
4. **Administrator Systemów Informatycznych (ASI)** – pracownik Działu Informatyki (DI), sprawujący nadzór techniczny w zakresie systemów teleinformatycznych, w tym bezpieczeństwa informacji, w tym danych osobowych przetwarzanych w systemach informatycznych.
5. **Baza danych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane.
6. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
7. **Droga elektroniczna, komunikacja elektroniczna** – poczta elektroniczna lub elektroniczna skrzynka podawcza, o której mowa w art. 3 pkt 17 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (t. j. Dz. U. z 2023 r. poz. 57).
8. **Dyrektor** – Dyrektor Powiatowego Zakładu Katastralnego we Wrocławiu.

9. **Działanie korygujące** – działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji.
10. **Działanie zapobiegawcze** – działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności / incydentu lub innej potencjalnej sytuacji niepożądanej.
11. **Hasło** – ciąg znaków literowych, cyfrowych i/lub specjalnych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
12. **Identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych i/lub specjalnych, jednoznacznie identyfikujących osobę upoważnioną.
13. **Incydent** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, w tym związanych ze zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego; naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
14. **Informacja niejawna** – informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zgodnie z ustawą z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (t. j. Dz. U. z 2023 r. poz. 756).
15. **Informacja stanowiąca tajemnicę służbową** – informacja uzyskana w związku z czynnościami służbowymi lub wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli, interesu publicznego lub jednostki.
16. **Inspektor Ochrony Danych (IOD)** – inspektor w rozumieniu art. 37 Rozporządzenia, osoba fizyczna powołana przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem rejestru zbiorów danych przetwarzanych przez administratora danych.
17. **Korekcja** - działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
18. **Moderator Systemu Informatycznego (MSI)** – Kierownik Pracowni Systemów Informacji Przestrzennej sprawujący nadzór techniczny w zakresie administracji uprawnieniami Systemu Informacji Przestrzennej Powiatu Wrocławskiego (wroSIP), w tym serwisu mapowego wroSIP, oraz uprawnieniami w portalu systemu teleinformatycznego Państwowego Zasobu Geodezyjnego i Kartograficznego (PZGiK), w tym w zakresie bezpieczeństwa informacji, w tym danych osobowych przetwarzanych w tych portalach.
19. **Niezgodność** – niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
20. **Nośniki danych** – przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych.
21. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane, w tym dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosownie do celów przetwarzania.

22. **Podatność** – luka (słabość), która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę.
23. **PBI / Polityka** – niniejszy dokument.
24. **Praca zdalna** - praca wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, m.in. z wykorzystaniem środków bezpośredniego porozumiewania się na odległość (całkowita lub hybrydowa).
25. **Pracownik** – osoba fizyczna świadcząca pracę na rzecz PZK na podstawie stosunku pracy, powołania, mianowania, wykonująca zadania wyłącznie osobiście, w ramach prowadzonej działalności gospodarczej lub powierzoną jej na podstawie umowy cywilnoprawnej, współpracująca w rozumieniu ustawy z dnia 13 października 1998 roku *o systemie ubezpieczeń społecznych* (t. j. Dz. U. z 2022 r. poz. 1009 ze zm.).
26. **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
27. **PZK** – Powiatowy Zakład Katastralny we Wrocławiu z siedzibą ul. Tadeusza Kościuszki 131, 50-440 Wrocław.
28. **PZGiK** – państwowy zasób geodezyjny i kartograficzny, prowadzony przez starostę przy pomocy geodety powiatowego, gromadzony w ośrodku dokumentacji geodezyjnej i kartograficznej na podstawie ustawy z dnia 17 maja 1989 r. *Prawo geodezyjne i kartograficzne (t. j. Dz. U. z 2021 r. poz. 1990 ze zm.)*. Czynności techniczne zadań Starosty Powiatu Wrocławskiego w zakresie państwowego zasobu geodezyjnego i kartograficznego realizuje PZK.
29. **Przetwarzane danych** – oznacza operację lub zestaw operacji wykonywanych na danych, w tym danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
30. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych).
31. **Słabość systemu** – zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu**.**
32. **System informatyczny / system IT** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania informacji, w tym danych osobowych.
33. **System teleinformatyczny PZGiK (system PZGiK)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, zintegrowany z portalami systemu teleinformatycznego PZGiK, służący do przetwarzania i udostępniania danych państwowego zasobu geodezyjnego i kartograficznego. Dane udostępniane za pomocą portali systemu PZGiK są replikowane z bazy źródłowej w wybranym – ograniczonym zakresie.

34. **System tradycyjny** – zespół procedur organizacyjnych, wyposażenia i środków trwałych związanych z mechanicznym przetwarzaniem informacji, w tym danych osobowych na nośnikach papierowych.
35. **Serwisant** – pracownik firmy zewnętrznej realizujący zadania związane z instalacją, naprawą lub konserwacją urządzeń technicznych, w tym sprzętu komputerowego, a także pracownik PZK, w którego zakresie obowiązków leży utrzymanie w sprawności technicznej urządzeń, w tym bieżące monitorowanie ich działania, diagnozowanie oraz eliminacja drobnych usterek i uszkodzeń.
36. **Sieć publiczna** – sieć telekomunikacyjna (WAN) wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych.
37. **Sieć wewnętrzna** – wewnętrzna sieć firmowa (LAN), w której uwierzytelnianie i kontrola dostępu do danych jest wykonywana za pomocą Active Directory (AD).
38. **Sytuacja kryzysowa** – sytuacja wpływająca negatywnie na poziom bezpieczeństwa zasobów i infrastruktury technicznej PZK, w tym każde zdarzenie, zagrożenie lub domniemanie utraty poufności, integralności lub dostępności informacji wrażliwej przetwarzanej w systemie teleinformatycznym.
39. **SZBI** – System Zarządzania Bezpieczeństwem Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu.
40. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
41. **UODO (Urząd Ochrony Danych Osobowych)** – organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych.
42. **Usuwanie danych** – zniszczenie danych lub modyfikacja danych osobowych, która uniemożliwi ustalenie tożsamości osoby, której dotyczą.
43. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
44. **Użytkownik** – pracownik PZK bez względu na rodzaj stosunku pracy i wymiar etatu, stażysta, praktykant oraz każda inna osoba, która uzyskała upoważnienie od ADO do przetwarzania danych osobowych.
45. **Użytkownik zewnętrzny** - osoba upoważniona przez kierownika podmiotu, z którym została podpisana umowa na korzystanie z portalu systemu teleinformatycznego PZGiK, umowa powierzenia przetwarzania danych osobowych lub inna umowa, na podstawie której następuje powierzenie przetwarzania danych osobowych.
46. **wroSIP** – System Informacji Przestrzennej Powiatu Wrocławskiego, utworzony na podstawie „Porozumienia w sprawie wspólnej budowy Systemu Informacji Przestrzennej Powiatu Wrocławskiego wroSIP" z dnia 3 listopada 2004 roku.
47. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i rozwiązań organizacyjnych zapewniających ochronę danych, w tym danych osobowych przed ich nieuprawnionym przetwarzaniem w systemie informatycznym.
48. **Zagrożenie** – potencjalna możliwość wystąpienia incydentu.
49. **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
50. **Zdarzenie** – błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z zagrożeniem bezpieczeństwa informacji, w tym danych osobowych.

§ 3.

1. Polityka Bezpieczeństwa Informacji jest dokumentem regulującym zasady przetwarzania i ochrony informacji, w tym danych osobowych w Powiatowym Zakładzie Katastralnym we Wrocławiu.
2. Celem PBI jest uzyskanie zgodnego z wymogami obowiązującego prawa sposobu przetwarzania informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu, zgodnie z zasadami wynikającymi z Rozdziału II RODO, w tym zapewnienie ochrony danych osobowych.

§ 4.

1. PBI określa w szczególności:
   1) prawa i obowiązki oraz granice dopuszczalnego zachowania Użytkowników systemów IT i Użytkowników zewnętrznych oraz konsekwencje naruszenia przepisów o ochronie danych osobowych;
   2) sposób przetwarzania informacji, w tym danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę tych danych;
   3) podstawowe warunki techniczne i organizacyjne jakim powinien odpowiadać system tradycyjny oraz system IT służący do przetwarzania informacji, w tym danych osobowych;
   4) wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych;
   5) instrukcję postępowania w sytuacji naruszenia ochrony informacji, w tym danych osobowych;
   6) zasady prowadzenia wykazu pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są informacje, w tym dane osobowe;
   7) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu informacji, w tym danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że informacje, w tym dane osobowe nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że informacje, w tym dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej;
   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania informacji, w tym danych osobowych.

Rozdział 2.
Zasady przetwarzania danych osobowych.
Powierzenie. Udostępnianie. Obowiązek informacyjny. Zgoda. Zabezpieczenia. Odpowiedzialność.

§ 5.

1. Zasady przetwarzania danych osobowych:
   1) dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. PZK może żądać podania jedynie tych danych, które są niezbędne do realizacji celów i zadań zakładu;
   2) zakres przetwarzanych danych osobowych nie może być szerszy niż powierzony do przetwarzania w związku z wykonywanymi obowiązkami;
   3) po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. Zasady ochrony informacji, w tym danych osobowych określone przez PBI mają zastosowanie do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów przetwarzania informacji, zawierających dane osobowe podlegające ochronie, w tym systemów IT;
   2) informacji będących własnością oraz przetwarzanych przez PZK w związku z realizacją celów i zadań;
   3) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
   4) wszystkich osób świadczących pracę lub wykonujących czynności na rzecz PZK, mających dostęp do informacji podlegających ochronie.

§ 6.

Przetwarzanie informacji, w tym danych osobowych w PZK odbywa się z wykorzystaniem:

1) dokumentów, materiałów, przesyłek analogowych tj. nieelektronicznych wniosków, zgłoszeń prac geodezyjnych i kartograficznych, dokumentacji stanowiącej podstawę zmian w operacie ewidencyjnym oraz dokumentów wchodzących w skład operatów technicznych, pism kierowanych do PZK, akt osobowych pracowników, dokumentów finansowo-księgowych, podań, dokumentów Zakładowego Funduszu Świadczeń Socjalnych (ZFŚS) i innych nośników systemu tradycyjnego;
2) danych zawartych na nośnikach danych magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych oraz danych przetwarzanych w:
   a) systemie teleinformatycznym państwowego zasobu geodezyjnego i kartograficznego (system PZGiK),
   b) systemie kadrowo-płacowym wykorzystywanym w PZK,
   c) systemie do obsługi dokumentów ubezpieczeniowych i wymianie informacji z ZUS,
   d) Systemie Informacji Przestrzennej Powiatu Wrocławskiego (wroSIP),
   e) systemach teleinformatycznych administracji (EKW, CEIDG, KRS, ZSiN, ePUAP).

§ 7.

1. Obszarem przetwarzania informacji, w tym danych osobowych są wydzielone pomieszczenia lub części pomieszczeń w siedzibie PZK znajdującej się przy ul. Tadeusza Kościuszki 131 we

Wrocławiu oraz miejsca pracy zdalnej. Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi **Załącznik nr 1 do PBI**. W przypadku Użytkowników zewnętrznych obszar przetwarzania danych określa kierownik podmiotu, z którym zawarta została umowa na korzystanie z portali, lub inna umowa, na podstawie której następuje powierzenie przetwarzania danych osobowych.

2. Pomieszczenia znajdujące się w budynku PZK podzielone są na dwie strefy:
   1) strefę administracyjną obejmującą pomieszczenia, gdzie kontrolowany jest ruch osobowy i materiałowy. Dostęp do tych pomieszczeń posiadają pracownicy PZK upoważnieni do pobierania klucza do danego pomieszczenia;
   2) strefę bezpieczeństwa obejmującą pomieszczenia objęte szczególną ochroną w celu uniemożliwienia osobom nieuprawnionym dostępu do pomieszczeń w tej strefie. Strefa bezpieczeństwa obejmuje archiwum zakładowe, kasę, serwerownię, pomieszczenie kadrowe, pomieszczenia techniczne.

§ 8.

Wykaz zbiorów danych osobowych wraz ze wskazaniem systemów zastosowanych do przetwarzania tych danych, podstawy przetwarzania opis struktury zbiorów danych oraz nazwy systemu informatycznego stanowi **Załącznik nr 2 do PBI**.

§ 9.

1. Wszyscy Pracownicy, którzy przetwarzają informacje, w tym dane osobowe muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez ADO **.** Wzór upoważnienia stanowi **Załącznik nr 3 do PBI**.
2. Wszyscy Pracownicy, którzy przetwarzają informacje, w tym dane osobowe zobowiązane są do złożenia oświadczenia o zachowaniu poufności, które warunkuje przydzielenie stosownych uprawnień do ich przetwarzania. Wzór oświadczenia o zachowaniu poufności stanowi **Załącznik nr 4 do PBI**.
3. W przypadku Użytkowników zewnętrznych upoważnienia do przetwarzania informacji, w tym danych osobowych nadaje kierownik podmiotu.

§ 10.

1. Uprawnienia do przetwarzania informacji, w tym danych osobowych w systemach IT nadawane są zgodnie z właściwą procedurą określoną w SZBI. Wzór wniosku o nadanie uprawnień dla użytkownika systemu informatycznego stanowi **Załącznik nr 3 do SZBI**.
2. Uprawnienia do przetwarzania informacji, w tym danych osobowych w portalu systemu teleinformatycznego PZGiK oraz systemie wroSIP dla Użytkowników zewnętrznych nadawane są zgodnie z właściwą procedurą określoną w SZBI. Wzory wniosków o wystąpienie o nadanie uprawnień dla Użytkownika zewnętrznego stanowią **Załączniki 4 -8 do SZBI** oraz Wniosek o udostępnienie danych zawartych w rejestrze publicznym, zgodny z rozporządzenia Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. z 2018 r. poz. 29).
3. Uprawnienia, o których mowa w ust. 1 niniejszego paragrafu, ważne są do dnia odwołania lub do chwili ustania zatrudnienia upoważnionego pracownika.

§ 11.

1. Ochrona dotyczy w szczególności informacji, w tym danych osobowych:

1) gromadzonych i przetwarzanych w dokumentach stanowiących podstawę zmian w operacie ewidencyjnym oraz wniosków i zgłoszeń prac, zgodnie z ustawą z dnia 17 maja 1989 r. *Prawo geodezyjne i kartograficzne*;
2) gromadzonych i przetwarzanych w związku z prowadzonymi zamówieniami publicznymi;
3) pracowników PZK, w tym danych zawartych w treści zawieranych umów o pracę;
4) kandydatów do pracy zbieranych na etapie rekrutacji;
5) zawartych w dokumentach finansowo-księgowych;
6) zawartych w dokumentach przekazywanych PZK do realizacji zadań statutowych;
7) dotyczących zabezpieczenia danych, w tym w szczególności identyfikatorów Użytkownika i haseł w systemach IT, w których są przetwarzane te dane;
8) zawartych w rejestrze osób dopuszczonych do przetwarzania.

§ 12.

1. W zbiorach danych gromadzonych w systemach IT zabrania się przetwarzania danych ujawniających:
   1) stan zdrowia;
   2) pochodzenie rasowe lub etniczne;
   3) poglądy polityczne;
   4) przekonania religijne lub filozoficzne;
   5) przynależność wyznaniową;
   6) przynależność partyjną lub związkową;
   7) dane genetyczne;
   8) dane biometryczne;
   9) nałogi;
   10) preferencje seksualne

   - chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę.
2. Dane o skazaniach, w tym dane o niekaralności można przetwarzać wyłącznie w zakresie uregulowanym w art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. *o Krajowym Rejestrze Karnym* (t. j. Dz. U. z 2023 poz.159).
3. Do profilowania zabrania się używania danych wymienionych w ust. 1 niniejszego paragrafu chyba, że wymagają tego obowiązujące przepisy prawa, osoba, której dane dotyczą wyraziła na to zgodę lub jest to podyktowane ważnym interesem publicznym.
4. Przy profilowaniu Administrator Danych Osobowych obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.
5. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą.
6. Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

§ 13.

Powierzenie przetwarzania danych osobowych.

1. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie pracownicy podmiotów (procesorów) świadczących usługi w związku z realizacją statutowych zadań PZK.

2. Powierzenie przetwarzania danych osobowych następuje na podstawie umowy zawartej w formie pisemnej lub równoważnej jej formie elektronicznej Wzór umowy powierzenia przetwarzania danych osobowych stanowi **Załącznik nr 13 do PBI**.
3. Zgodnie z art. 28 RODO, umowa powierzenia danych osobowych powinna określać przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy (administratora i procesora).
4. Zakres powierzanych danych osobowych powinien być adekwatny do celu powierzenia.
5. Administrator danych osobowych zobowiązany jest do dokumentowania powierzania tych danych w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi. Wzór wykazu podmiotów, którym powierzono dane osobowe stanowi **Załącznik nr 8 do PBI**. Za prowadzenie wykazu odpowiedzialny jest Kierownik Działu Ogólno-Administracyjnego.
6. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych), wymagana jest zgoda ADO na przekazanie powierzonych danych, wyrażona w formie pisemnej lub równoważnej jej formie elektronicznej.
7. Umowa powierzenia przetwarzania danych osobowych, o której mowa w ust. 2 podlega opiniowaniu przez IOD i ASI/MSI.
8. Administrator nie przekazuje danych osobowych do państw poza terenem Unii Europejskiej.

§ 14.
Udostępnianie danych osobowych

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności.
2. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych.
3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.
4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem RODO lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 15.
Obowiązek informacyjny

1. W przypadku zbierania danych osobowych od osoby (art. 13 RODO), której one dotyczą, ADO jest obowiązany poinformować tę osobę o:
   1) adresie swojej siedziby i pełnej nazwie;
   2) celu i zakresie zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

3) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej i konsekwencjach niepodania danych;
4) Inspektorze Ochrony Danych;
5) prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywać się będzie przetwarzanie danych;
6) okresie, przez który dane osobowe będą przechowywane lub o kryteriach tego okresu;
7) profilowaniu danych;
8) powierzaniu lub udostępnianiu danych osobowych;
9) prawach osoby, której dane dotyczą tj. prawie do usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych), prawie do złożenia skargi na działania administratora do Prezesa UODO.

2. W przypadku pozyskania danych osobowych z innego źródła (art. 14 RODO), niż osoba, której dane dotyczą, ADO jest dodatkowo zobowiązany poinformować tę osobę o źródle pozyskania danych.
3. Obowiązek poinformowania wymieniony w ust. 1 niniejszego paragrafu powinien być wykonany w momencie podjęcia pierwszej czynności w stosunku do podmiotu danych osobowych.

§ 16.

Zgoda na przetwarzanie danych osobowych.

1. Zgodnie z art. 4 pkt 11 RODO "zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
2. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana ani wynikać z oświadczenia woli o innej treści, tzn. zgoda nie może być zawarta np. w regulaminie, którego zaakceptowanie wiąże się ze zgodą na warunki w nim zawarte.
3. Zgodnie z motywem 32 RODO, w przypadku pozyskania zgody w formie innej niż pisemna, na ADO ciąży obowiązek udowodnienia, że została ona pozyskana, a nie dorozumiana.
4. Zgoda na przetwarzanie danych osobowych powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, należy pozyskać odrębną zgodę na każdy cel.
5. Zgodnie z motywem 32 RODO, elektroniczne pytanie o zgodę musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.
6. Zgodnie z art. 8 RODO, w przypadku dziecka, które nie ukończyło 16 roku życia, wymagana jest zgoda lub wyrażenie aprobaty osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem wyłącznie w zakresie wyrażonej zgody.
7. W przypadku opisanym w ust. 6 niniejszego paragrafu, ADO, uwzględniając dostępną technologię, jest zobowiązany do podjęcia rozsądnych starań w celu zweryfikowania, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.
8. Zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie w sposób tak samo prosty i przystępny, w jaki została pozyskana.

§ 17.

Zgoda na przetwarzanie danych osobowych nie jest wymagana w przypadku, gdy dane będą przetwarzane:

1) w związku z zawarciem umowy z osobą, której dane dotyczą;
2) na podstawie przepisu prawa;
3) w interesie publicznym;
4) w prawnie usprawiedliwionym celu administratora danych;
5) w przypadku żywotnego interesu osoby, której dane dotyczą, gdy pozyskanie zgody jest konieczne, ale niemożliwe.

§ 18.

Zabezpieczenia danych osobowych.

1. W celu zapewnienia należytej ochrony przetwarzania informacji oraz danych osobowych, w PZK stosuje się zabezpieczenia techniczne i organizacyjne, o których mowa od § 19 do § 23.
2. Dopuszcza się stosowanie również innych zabezpieczeń technicznych i organizacyjnych mających na celu podniesienie poziomu ochrony danych osobowych.

§ 19.

Zabezpieczenia techniczne.

1. Dokumenty zawierające dane osobowe w formie analogowej (papierowej), upoważnione osoby przechowują w obszarze przetwarzania danych w zabezpieczonych pomieszczeniach (zamki na klucz, karty zbliżeniowe).
2. Pomieszczenia, w których przetwarzane są informacje, w tym dane osobowe są zabezpieczone przed skutkami pożaru za pomocą instalacji przeciwpożarowej i oddymiania klatek schodowych.
3. Dostęp do pomieszczeń kontrolowany jest przez system całodobowego monitoringu wizyjnego.
4. W przypadku konieczności zniszczenia dokumentów analogowych (papierowych) zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce.
5. O ile to możliwe należy stosować urządzenia typu UPS, generator prądu lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
6. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są informacje, w tym dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora Użytkownika (loginu) oraz hasła.
7. Stosowany system informatyczny posiada mechanizm wymuszający okresową zmianę haseł dostępu.
8. Dla potrzeb ochrony danych stosuje się środki ochrony przed szkodliwym oprogramowaniem.
9. Do ochrony dostępu do sieci komputerowej stosuje się zaporę sieciową (system Firewall).
10. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
11. Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych.
12. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy Użytkownika.

§ 20.

Zabezpieczenia organizacyjne

1. Opracowano i wdrożono *Politykę Bezpieczeństwa Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu* oraz SZBI.
2. Powołano *Inspektora Ochrony Danych*, który sprawuje nadzór nad przetwarzaniem danych osobowych.
3. *Administrator Systemów Informatycznych* oraz *Moderator Systemów Informatycznych*, sprawują nadzór techniczny w zakresie systemów teleinformatycznych, w tym bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.
4. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie oraz które podpisały oświadczenie o zachowaniu poufności.
5. Prowadzone są wykazy osób i podmiotów, którym udostępniono lub powierzono przetwarzanie danych osobowych.
6. Wszyscy Użytkownicy wykonujący czynności związane z przetwarzaniem danych osobowych zostali zaznajomieni z przepisami dotyczącymi ochrony tych danych.
7. Wszyscy Użytkownicy systemów informatycznych zostali przeszkoleni w zakresie zasad korzystania i zabezpieczeń tych systemów.
8. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.
9. Przetwarzane danych osobowych przez Użytkowników odbywa się w wyznaczonych pomieszczeniach, zgodnie ze strefami kontroli, w godzinach pracy PZK lub po godzinach po uprzednim uzyskaniu zgody ADO.
10. Praca zdalna odbywa się w miejscu i w czasie uzgodnionym między pracownikiem i ADO.
11. Praca zdalna może odbywać się wyłącznie na autoryzowanym przez ASI komputerze lub urządzeniu mobilnym. Łączność z siecią komputerową PZK może się odbywać jedynie poprzez połączenie kablowe ethernet lub WIFI zabezpieczone protokołem co najmniej WPA2-PSK.
12. Dostęp osób nieposiadających stosownych upoważnień do pomieszczeń, w których przetwarzane są dane osobowe odbywa się wyłącznie za zgodą ADO lub w obecności osób upoważnionych.
13. Wszystkie osoby przetwarzające dane osobowe zobowiązane są do zachowania tajemnicy poprzez złożenie pisemnego oświadczenia o zachowaniu poufności.
14. Wykonywane kopie zapasowe zbiorów danych osobowych przechowywane są dodatkowo w pomieszczeniu innym niż to, w którym znajduje się serwer, na którym dane przetwarzane są na bieżąco.

§ 21.

1. Wszyscy pracownicy świadczący pracę na rzecz PZK na podstawie stosunku pracy, posiadający dostęp do danych osobowych, uczestniczą w cyklicznych szkoleniach (minimum raz w roku) z zakresu przepisów prawa dotyczących ochrony danych osobowych oraz regulacji wewnętrznych obowiązujących w PZK. Szkolenia przeprowadza IOD we współpracy z Działem Ogólno-Administracyjnym i ASI/MSI.
2. Zakres czynności osoby upoważnionej do przetwarzania danych osobowych określa zakres odpowiedzialności tej osoby za ochronę przetwarzanych danych osobowych w stopniu adekwatnym do jej zadań na stanowisku pracy.
3. Pracownicy świadczący pracę na rzecz PZK na podstawie stosunku pracy, przebywając w siedzibie zakładu, są zobowiązani do noszenia w widocznym miejscu identyfikatora

upoważniającego do przebywania w strefie administracyjnej. Identyfikator zawiera imię i nazwisko pracownika, nazwę komórki organizacyjnej i stanowisko pracy. Identyfikatory wydaje Dział Ogólno-Administracyjny.

4. Pracownicy świadczący pracę zdalną na rzecz PZK na podstawie stosunku pracy, przebywając poza siedzibą zakładu, są zobowiązani do zabezpieczenia swojego miejsca pracy przed dostępem osób trzecich do danych osobowych.
5. Praktykanci, stażyści i inne osoby upoważnione do przebywania w strefie administracyjnej zobowiązane są do noszenia identyfikatora zawierającego imię i nazwisko oraz stosowne oznaczenie wynikające z realizowanych czynności/stanowiska. Identyfikatory wydaje Dział Ogólno-Administracyjny.
6. W przypadku utraty ważności upoważnienia do przebywania w strefie administracyjnej na skutek ustania stosunku pracy, zakończenia praktyki, stażu lub wizyty, identyfikator podlega zwrotowi do Działu Ogólno-Administracyjnego.
7. Zgubienie lub utratę identyfikatora należy niezwłocznie zgłosić Działu Ogólno-Administracyjnego wraz z wyjaśnieniem okoliczności zdarzenia.

§ 22.

1. Ze względu na specyfikę realizowanych działań, w PZK nie prowadzi się ewidencji osób przebywających w siedzibie zakładu w godzinach i poza godzinami urzędowania, z wyjątkiem list obecności pracowników świadczący pracę na rzecz PZK na podstawie stosunku pracy, a także praktykantów i stażystów. Szczegółowe godziny pracy i zasady przebywania w siedzibie PZK określa *Regulamin Pracy Powiatowego Zakładu Katastralnego we Wrocławiu*.
2. Nadzór nad dostępem do pomieszczeń strefy administracyjnej sprawują kierownicy poszczególnych komórek organizacyjnych, pracownicy Działu Ogólno-Administracyjnego oraz osoby upoważnione przez Dyrektora.
3. Nadzór nad dostępem do pomieszczeń strefy bezpieczeństwa sprawują osoby upoważnione przez Dyrektora.
4. Pracownicy są zobowiązani do informowania Działu Ogólno-Administracyjnego o zauważonych próbach nieuprawnionego dostępu do pomieszczeń wchodzących w skład strefy administracyjnej i bezpieczeństwa. O każdym takim incydencie powinien być niezwłocznie powiadomiony IOD, a samo zdarzenie odnotowane w *Rejestrze incydentów*.

§ 23.

1. Pobieranie i zdawanie kluczy do pomieszczeń strefy administracyjnej i bezpieczeństwa, odnotowuje się w systemie informatycznym przy użyciu kart bezstykowych RFID.
2. Listę osób upoważnionych do pobierania kluczy prowadzi Dział Ogólno-Administracyjny.
3. Wszystkie problemy związane z dostępem do strefy administracyjnej i bezpieczeństwa, w tym dotyczące kart bezstykowych RFID, kluczy itp. należy zgłaszać do Działu Ogólno-Administracyjnego.
4. Dostęp do pomieszczeń strefy administracyjnej po godzinach urzędowania PZK, mają osoby upoważnione przez Dyrektora oraz osoby sprzątające upoważnione przez administratora budynku.
5. Dyrektor w porozumieniu z IOD oraz ASI/MSI może określić pomieszczenia, do których dostęp osób sprzątających będzie ograniczony i możliwy tylko pod nadzorem osób upoważnionych.

6. Osoba opuszczająca jako ostatnia pomieszczenie, w którym przetwarzane są dane osobowe, zobowiązana jest do zamknięcia drzwi na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie, za wyjątkiem sytuacji związanych z ochroną przeciwpożarową.
7. Zabrania się samowolnego wykonywania kopii kluczy oraz ich wynoszenia poza siedzibę PZK. Każdorazowa potrzeba dorobienia dodatkowego klucza musi być zgłoszona do Działu Ogólno-Administracyjnego.
8. Po zakończeniu pracy pracownicy zobowiązani są do wylogowania z systemów informatycznych, zamknięcia okien w pomieszczeniu, umieszczenia dokumentów zawierających dane osobowe w szafach lub szufladach - zgodnie z zasadą *czystego biurka*, *czystej drukarki* i *czystej kopiarki* (o ile takie urządzenia znajdują się w pomieszczeniu) oraz zgodnie z *Instrukcją kancelaryjną* - zniszczenia w niszczarce wszystkich materiałów zbędnych, w postaci błędnie wytworzonej lub niepotrzebnej dokumentacji, mającej krótkotrwałe znaczenie praktyczne m.in. wydruków komputerowych i innych materiałów analogowych zawierających dane osobowe.

§ 24.

1. Udostępnianie drogą pocztową lub kurierską dokumentów i materiałów zawierających dane osobowe może odbywać się przesyłką rejestrowaną, a w przypadku danych zawartych na nośnikach magnetycznych, optycznych lub elektronicznych – przesyłką rejestrowaną za potwierdzeniem odbioru.
2. Pracownicy przygotowujący przesyłki, o których mowa w ust. 1 powinni dołożyć należytej staranności celem zabezpieczenia ich zawartości przed nieuprawnionym dostępem do ich zawartości osób trzecich.

§ 25.
Odpowiedzialność.

1. Za zapewnienie pracownikom warunków organizacyjnych mających na celu zachowanie należytego bezpieczeństwa informacji, w tym danych osobowych odpowiadają kierownicy poszczególnych komórek organizacyjnych lub przełożeni wyższego stopnia.
2. IOD we współpracy z ASI/MSI i Działem Ogólno-Administracyjnym w porozumieniu z kierownikami poszczególnych komórek organizacyjnych, zapewniają bieżącą edukację pracowników dotyczącą zasad bezpieczeństwa informacji, w tym danych osobowych przetwarzanych w systemach informatycznych i systemie tradycyjnym.
3. Na pracownikach oraz osobach upoważnionych do przetwarzania informacji, w tym danych osobowych, w zakresie ich uprawnień i odpowiedzialności, ciąży obowiązek dbałości o zabezpieczanie danych przed ich udostępnieniem, zabraniem, przetwarzaniem z naruszeniem ustawy przez osoby nieuprawnione oraz zmianą, uszkodzeniem, utratą lub zniszczeniem.
4. Kierownicy odpowiadają za przygotowanie Wniosku dotyczącego uprawnień dla użytkownika w systemie informatycznym zgodnie z zakresem obowiązków pracownika, jak również przygotowują wnioski o odebranie uprawnień w przypadku zmiany zakresu obowiązków pracownika - **Załącznik nr 3 do SZBI**.
5. Kierownicy komórek organizacyjnych PZK odpowiadają za nadzór nad użytkownikami w zakresie stosowania zasad wynikających z PBI.

§ 26.

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 107 *ustawy o ochronie danych osobowych*, administracyjną lub cywilną.
2. Odpowiedzialności karnej podlega każdy pracownik, który:

1) przetwarza w zbiorze danych dane osobowe, do których nie jest upoważniony;
2) przetwarza w zbiorze danych dane, których przetwarzanie jest zabronione;
3) przetwarza w zbiorze danych dane niezgodne z celem stworzenia tego lub innych zbiorów;
4) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
5) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
6) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw.

3. Złamanie zasad PBI stanowi incydent, o którym powinien być niezwłocznie powiadomiony IOD. O podjęciu działań następczych decyduje ADO na podstawie projektu działań naprawczych opracowanych przez IOD we współpracy z Działem Ogólno-Administracyjnym. W przypadku wystąpienia incydentu związanego z przetwarzaniem danych osobowych w systemach informatycznych, projekt naprawczy opracowuje i przedstawia IOD we współpracy z ASI/MSI.
4. Łamanie zasad wynikających z PBI może być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych i może skutkować nałożeniem kary porządkowej na zasadach określonych w przepisach prawa pracy oraz *Regulaminie Pracy Powiatowego Zakładu Katastralnego we Wrocławiu*, w szczególności w przypadku osoby, która po stwierdzeniu naruszenia bezpieczeństwa danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie Działu Ogólno-Administracyjnego.
5. Udokumentowane umyślne złamanie zasad określonych w PBI jest traktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia z winy pracownika.

Rozdział 3.
Administrator Danych Osobowych. Inspektor Ochrony Danych. Administrator Systemów Informatycznych. Moderator Systemu Informatycznego.

§ 27.
Administrator Danych Osobowych (ADO)

1. Do zadań Administratora Danych Osobowych należy podejmowanie decyzji w zakresie celów i środków przetwarzania informacji, w tym danych osobowych wynikających z powszechnie obowiązujących przepisów prawa.
2. Zadania nałożone przez RODO na ADO obejmują w szczególności:
   1) wypełnianie obowiązku informacyjnego przy zbieraniu danych osobowych (art. 24 i 25 rozporządzenia);
   2) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza (art. 26 rozporządzenia);
   3) udzielanie informacji o celu i zakresie przetwarzanych danych osobowych (art. 33 i 34 rozporządzenia);
   4) właściwego uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane (art. 35 ustawy);
   5) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (art. 36 ustawy);
   6) kontrolowanie jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane (art. 38 ustawy);

7) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).

3. ADO pełni funkcję kontrolną w zakresie poprawnego przetwarzania informacji, w tym danych osobowych zgodnie z wymogami i zaleceniami RODO, *ustawy o ochronie danych osobowych*. Zapewnia środki realizacji odpowiedniej ochrony informacji oraz nadzoruje przestrzeganie ustalonych zasad zawartych w PBI.

§ 28.

Inspektor Ochrony Danych (IOD)

IOD jest powoływany przez ADO drogą pisemnego upoważnienia. Wzór upoważnienia dla IOD stanowi **Załącznik nr 5 do PBI**. IOD jest również zobowiązany do podpisania oświadczenia o zachowaniu poufności stanowiący **Załącznik nr 4 do PBI**.

§ 29.

Do kompetencji IOD należy w szczególności:

1) sprawdzanie zgodności przetwarzania informacji, w tym danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdań dla ADO;
2) nadzorowanie przestrzegania zasad ochrony informacji, w tym danych osobowych tj. środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych informacji, w tym danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, ze szczególnym uwzględnieniem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w tym nadzór nad obiegiem oraz przechowywaniem materiałów i dokumentów zawierających dane osobowe we współpracy z ASI/MSI;
3) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania informacji, w tym danych osobowych, środki ich ochrony oraz przestrzegania zasad w niej określonych;
4) wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych oraz pozostałych wniosków dotyczących bezpieczeństwa informacji, w tym danych osobowych, a także nadzór w zakresie realizacji tych wniosków;
5) nadzór nad fizycznym zabezpieczeniem pomieszczeń we współpracy z ADO, w których przetwarzane są informacje, w tym dane osobowe oraz organizacją kontroli przebywających w nich osób;
6) zapewnienie przeciwdziałania incydentów oraz prowadzenie rejestru incydentów i zagrożeń (**Załącznik nr 10 do PBI**);
7) w porozumieniu z ASI/MSI, szkolenie osób upoważnionych do przetwarzania informacji, w tym danych osobowych w zakresie przepisów o ochronie danych osobowych oraz zapewnienie bieżącej edukacji Użytkowników w zakresie polityki bezpieczeństwa, w tym wnioskowanie do ADO w zakresie szkoleń dotyczących polityki bezpieczeństwa.

§ 30.

1. Dział Ogólno-Administracyjny we współpracy ASI/MSI prowadzi rejestr przetwarzania zbiorów danych osobowych (**Załącznik nr 14 do PBI**), w którym odnotowywane są udostępnienia do przetwarzania.

2. W ramach nadzoru nad przetwarzaniem danych, IOD we współpracy z Działem Ogólno-Administracyjnym weryfikuje w szczególności cel i zakres przetwarzania, okres przetwarzania oraz sposoby zabezpieczenia danych osobowych.
3. IOD we współpracy z ASI/MSI jest również zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym.
4. IOD we współpracy z Działem Ogólno-Administracyjnym prowadzi następujące wykazy:
   1) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (**Załącznik nr 1 do PBI**);
   2) wykaz osób, którym nadano upoważnienia do przetwarzania danych osobowych (**Załącznik nr 6 do PBI**);
   3) wykaz udostępnień danych osobowych innym podmiotom (**Załącznik nr 7 do PBI**);
   4) wykaz podmiotów, którym powierzono dane osobowe do przetwarzania (**Załącznik nr 8 do PBI**);
   5) wykaz udostępnień danych osobowych osobom, których dane dotyczą (**Załącznik nr 9 do PBI**).

§ 31.
Administrator Systemów Informatycznych (ASI)

1. Do zadań ASI należy aktywny udział w rozwijaniu infrastruktury teleinformatycznej, ze szczególnym uwzględnieniem potrzeby stałego podnoszenia poziomu bezpieczeństwa systemów IT i danych wynikający z obowiązujących przepisów, PBI oraz zaleceń IOD.
2. Współpraca przy nadzorowaniu przez IOD przestrzegania bezpieczeństwa informacji, w tym danych osobowych gromadzonych i przetwarzanych w systemach IT, ma na celu zabezpieczenie ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Do kompetencji ASI należy w szczególności:
   1) przydzielanie uprawnień dostępu do systemów teleinformatycznych, w tym danych i usług, oraz dostępu do poczty elektronicznej oraz współpraca przy kontroli dostępu do danych osobowych;
   2) inicjatywa w zakresie zapewnienia alternatywnego, awaryjnego zasilania systemów informatycznych oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, w tym raportowanie do ADO stanu zabezpieczeń w zakresie awaryjnego zasilania, w porozumieniu z Działem Ogólno-Administracyjnym i administratorem budynku;
   3) podejmowanie działań zabezpieczających systemy informatyczne w przypadku otrzymania informacji o naruszeniu zabezpieczeń bądź informacji o zmianach w sposobie działania systemów wskazujących na naruszenie bezpieczeństwa danych;
   4) uczestniczenie w procesie zapewnienia ochrony systemów teleinformatycznych oraz danych osobowych przesyłanych za pośrednictwem tych systemów;
   5) uczestniczenie w procesie zapewnienia ochrony danych osobowych w związku z naprawą, konserwacją oraz likwidacją systemów informatycznych, w tym urządzeń komputerowych, na których zapisane są dane osobowe;
   6) wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych w systemach informatycznych oraz realizacja tych czynności po akceptacji ADO;

7) zapewnienie możliwości przeglądów, konserwacji oraz uaktualnień systemów służących do przetwarzania danych osobowych przez serwisantów;
8) inicjatywa w zakresie poprawy organizacji pracy mających wpływ na bezpieczeństwo przetwarzania informacji, w tym w zakresie przepisów bhp i ppoż.

§ 32.
Moderator Systemu Informatycznego (MSI)

1. Do zadań MSI należy administracja uprawnieniami w portalu systemu teleinformatycznego państwowego zasobu geodezyjnego i kartograficznego (portal PZGiK) oraz systemie wroSIP.
2. Do kompetencji MSI należy w szczególności:
   1) aktywny udział w stałym podnoszeniu poziomu bezpieczeństwa w administrowanym portalu systemu PZGiK oraz systemie wroSIP, w tym danych osobowych w nich przetwarzanych, w porozumieniu z IOD i ASI oraz dostawcami wykorzystywanych rozwiązań;
   2) uczestniczenie w porozumieniu z dostawcami portalu systemu PZGiK i wroSIP w procesie zapewnienia mechanizmów uwierzytelniania Użytkowników i Użytkowników zewnętrznych, w których przetwarzane są informacje, w tym dane osobowe, oraz kontroli dostępu do danych osobowych;
   3) uczestniczenie w procesie zapewnienia ochrony danych osobowych przetwarzanych w portalu systemu PZGiK i systemie wroSIP, w tym podjęcie działań zabezpieczających w przypadku otrzymania informacji o naruszeniu zabezpieczeń, informacji o zmianach w sposobie działania portali lub systemu wskazujący na naruszenie bezpieczeństwa danych;
   4) uczestniczenie w procesie zapewnienia ochrony danych osobowych w związku z naprawą, konserwacją oraz likwidacją portali i systemu wroSIP;
   5) wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych w portalach i systemie wroSIP oraz realizacja tych czynności po akceptacji ADO.

Rozdział 4.
Ogólne warunki korzystania z systemu informatycznego.

§ 33.

1. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji, w tym danych osobowych przed ich nieuprawnionym przetwarzaniem.
2. Każdy Użytkownik systemu informatycznego stosowanego w PZK jest zobowiązany do zapoznania się z zasadami korzystania z tego systemu.
3. Korzystanie z funkcjonalności systemu informatycznego jest możliwe pod warunkiem złożenia do ADO *Wniosku o nadanie/modyfikację/cofnięcie uprawnień dla użytkownika systemu informatycznego*. Wzór stanowi **Załącznik nr 3 do SZBI**.
4. Korzystanie z funkcjonalności obejmujących wgląd do danych osobowych w portalu Systemu Informacji Przestrzennej Powiatu Wrocławskiego wroSIP (portal wroSIP) oraz portalu systemu teleinformatycznego państwowego zasobu geodezyjnego i kartograficznego (portal PZGiK) jest możliwe po spełnieniu warunków:
   a) w przypadku Użytkownika – akceptacji przez ADO *Wniosku o nadanie/modyfikację/cofnięcie uprawnień dla użytkownika systemu informatycznego*. Wzór stanowi **Załącznik nr 3 do SZBI**.

b) w przypadku Użytkownika zewnętrznego - zawarcie z ADO umowy na korzystanie z portali lub innej umowy, na podstawie której następuje powierzenie przetwarzania danych osobowych. Zawarcie umowy na korzystanie z portali poprzedzone jest złożeniem odpowiedniego wniosku (**Załączniki 4-8 do SZBI** lub Wniosek o udostępnienie danych zawartych w rejestrze publicznym, zgodny z rozporządzeniem Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. z 2018 r. poz. 29).

5. Szczegółowe procedury nadawania uprawnień do systemów informatycznych określa SZBI.

§ 34.

1. Wykaz osób upoważnionych do przetwarzania danych osobowych stanowi Załącznik nr 6 do PBI. Wykaz nie obejmuje osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych umożliwiających elektroniczne prowadzenie ewidencji, za które odpowiada ASI/MSI.
2. Ewidencję osób posiadających uprawnienia do przetwarzania danych osobowych w zakresie portalu systemu PZGiK oraz systemu wroSIP prowadzi MSI. Ewidencja prowadzona w wersji elektronicznej w pliku LISTA_UZYTKOWNIKOW.XLS obejmuje informacje stanowiące **Załącznik nr 11 do SZBI.**
3. Plik, o którym mowa w ust. 2 jest odpowiednio zabezpieczony poprzez szyfrowanie (hasło) oraz lokalizację na serwerze, z którego wykonywane są regularne kopie bezpieczeństwa. Dostęp do pliku posiadają wyłącznie administratorzy systemów oraz osoby odpowiedzialne za nadzorowanie czynności związanych z bezpieczeństwem informacji w PZK.

§ 35.

1. Zabrania się Użytkownikowi i Użytkownikowi zewnętrznemu podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń systemów.
2. W celu zapobieżenia nieautoryzowanemu dostępowi do systemów informatycznych Użytkownik i Użytkownik zewnętrzny nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom.
3. Zabronione jest korzystanie z systemów informatycznych z użyciem danych dostępowych innego Użytkownika lub Użytkownika zewnętrznego.
4. Użytkownicy i Użytkownicy zewnętrzni są zobowiązani do ustawienia monitorów ekranowych w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
5. Użytkownik i Użytkownik zewnętrzny zobowiązany jest do przestrzegania zasady „czystego biurka", w szczególności przed opuszczeniem swego stanowiska pracy powinien schować wszelkie dokumenty oraz informatyczne nośniki danych.
6. W czasie kopiowania, drukowania dokumentów zawierających dane osobowe, Użytkownik i Użytkownik zewnętrzny zobowiązany jest do zachowania zasady „czystej drukarki", „czystej kopiarki", w szczególności przed opuszczeniem stanowiska kopiowania/drukowania upewnić się, że w urządzeniach nie pozostały dokumenty zawierające dane osobowe.
7. Przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, Użytkownik i Użytkownik zewnętrzny jest zobowiązany do sprawdzenia, czy posiadane przez niego dane były należycie zabezpieczone oraz, czy zabezpieczenia te nie były naruszone.

8. Po zakończeniu przetwarzania danych osobowych, Użytkownik i Użytkownik zewnętrzny zobowiązany jest do należytego zabezpieczenia ich przed dostępem osób nieupoważnionych.

Rozdział 5.
Poczta elektroniczna.

§ 36.

1. Użytkownik zobowiązany jest do dbania o bezpieczeństwo służbowego konta poczty elektronicznej, w szczególności do:
   1) używania silnego hasła dostępu;
   2) nieotwierania załączników do poczty i linków pochodzących z podejrzanych źródeł;
   3) zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.
2. Za zachowanie bezpieczeństwa systemów informatycznych służących do obsługi poczty elektronicznej odpowiada zewnętrzny dostawca usługi.
3. Szczegółowe procedury korzystania z poczty elektronicznej oraz zasady konfiguracji sprzętu komputerowego Użytkownika systemu informatycznego reguluje SZBI.

§ 37.

1. W stosunku do pozostałych informacji przetwarzanych w związku z realizacją zadań statutowych PZK, stosuje się zasady bezpieczeństwa określone w ustawie z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (t. j. Dz. U. z 2019 r. poz. 742 z późn. zm.).
2. Wymagania w zakresie dostępu oraz zabezpieczenia pozostałych informacji i danych określa *Regulamin organizacyjny Powiatowego Zakładu Katastralnego we Wrocławiu*.

Rozdział 6.
Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych.

§ 38.

1. Ryzyko w zakresie bezpieczeństwa informacji, w tym danych osobowych, definiuje się jako prawdopodobieństwo wystąpienia zagrożeń i powstanie szkód, zniszczeń oraz przerw lub zakłóceń prawidłowego funkcjonowania systemu tradycyjnego oraz systemów informatycznych, w których przetwarzane są dane osobowe.
2. Zarządzanie ryzykiem jest procesem identyfikacji zasobów, odpowiadających im podatności i zagrożeń, oceny prawdopodobieństwa ich wystąpienia, wielkości potencjalnych strat oraz przeciwdziałania i określenia kryteriów akceptowalności ryzyka. Proces ten obejmuje:
   1) możliwie jak najszybszą identyfikację ryzyka związanego z planowanym działaniem;
   2) ocenę stopnia wpływu ryzyka na uzyskane wyniki lub cele PZK;
   3) zastosowanie odpowiednich środków kontroli ryzyka.
3. Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, odnoszącym się do zadań PZK, dokonywany jest do końca I kwartału bieżącego roku kalendarzowego przez IOD, przy wsparciu Działu Ogólno-Administracyjnego oraz ASI/MSI w zakresie systemów informatycznych.
4. Narzędziem wsparcia w tym zakresie jest *Arkusz zarządzania ryzykiem* zawierający ryzyka zidentyfikowane dla PZK. Wzór arkusza stanowi **Załącznik nr 15 do PBI**.

5. Kierownicy komórek organizacyjnych oraz pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko. Lista możliwych do zastosowania mechanizmów kontroli redukujących ryzyko stanowi **Załącznik nr 16 do PBI**.
6. Wypełnione arkusze zarządzania ryzykiem przekazywane są do IOD. Na ich podstawie IOD, w przypadku ryzyk dotyczących bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych w porozumieniu z ASI/MSI, opracowuje roczne sprawozdania, które w postaci raportu o zidentyfikowanych ryzykach przekazuje ADO.

§ 39.

1. Niezależnie od corocznej oceny ryzyk, IOD we współpracy Działem Ogólno-Administracyjnym oraz ASI/MSI, przeprowadza ocenę ryzyk po każdorazowym wystąpieniu incydentu oraz każdorazowej zmianie mogącej wpływać na poziom ryzyka, w tym szczególnie zmianie:
   1) struktury organizacyjnej;
   2) otoczenia dotyczącego realizacji umów z nowymi podmiotami;
   3) technologii, infrastruktury, pracowników, metod pracy;
   4) przepisów prawa.
2. Niezwłocznie po wystąpieniu incydentu, IOD w porozumieniu z ASI/MSI przedstawia ADO wyniki oceny zidentyfikowanych ryzyk wraz z propozycjami działań korygujących i zapobiegawczych, do których należy w szczególności: określenie zadań do realizacji, zdefiniowanie odpowiedzialności, ram czasowych oraz propozycji zmian celem poprawy bezpieczeństwa informacji.
3. Na podstawie raportów i sprawozdań otrzymanych od IOD, ADO podejmuje ostateczną decyzję w zakresie realizacji działań zapewniających ochronę przetwarzanych informacji.
4. Do działań wskazanych w ust. 3 należy w szczególności:
   1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
   2) utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
   3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
   4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
   5) dokonanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
   6) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
      a) zagrożenia bezpieczeństwa informacji,
      b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
      c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich;

7) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy zdalnej;
9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawieranie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację systemu operacyjnego,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i PBI;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

§ 40.

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   1) próby naruszenia ochrony danych:
      a) z zewnątrz - włamania do systemu, podsłuch, kradzież danych,
      b) z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych;
   2) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne;
   3) awarie sprzętu lub uszkodzenie oprogramowania;
   4) zabór sprzętu lub nośników z ważnymi danymi;

5) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych;
6) usiłowanie zakłócenia działania systemu informatycznego..

2. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   2) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
   4) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   5) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
   6) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:
   1) zgłoszenia od Użytkowników;
   2) alarmy z systemów informatycznych;
   3) analizy incydentów;
   4) wyniki audytów / kontroli.

§ 41.

Każdy pracownik, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować IOD poprzez Dział Ogólno-Administracyjny. Zasady działania w takich przypadkach określa **tabela nr 1:**

Tabela nr 1.

Zasady działania w przypadku zagrożenia lub naruszenia ochrony danych osobowych

Kod uchybienia lub zagrożenia	Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru	Należy zabezpieczyć dane osobowe oraz powiadomić IOD poprzez Dział Ogólno-Administracyjny, który powiadamia ADO przekazując *Protokół uchybienia* (**Załącznik nr 11 do PBI**).
2	Komputer nie jest zabezpieczony hasłem	Należy zabezpieczyć dane osobowe oraz powiadomić IOD poprzez Dział Ogólno-Administracyjny, który powiadamia ASI. IOD we współpracy z ASI, powiadamia ADO przekazując *Protokół uchybienia*.
3	Dostęp do danych mają osoby nieupoważnione	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD poprzez Dział Ogólno-Administracyjny.

		IOD powiadamia ADO przekazując *Protokół uchybienia*.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Należy powiadomić IOD poprzez Dział Ogólno-Administracyjny, który we współpracy z ASI/MSI powinien sprawdzić system uwierzytelniania oraz czy nie doszło do kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI/MSI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Należy nie dopuścić do kradzieży danych i powiadomić IOD i ASI/MSI poprzez Dział Ogólno-Administracyjny. ASI/MSI w porozumieniu z IOD powinien zabezpieczyć nośnik danych. IOD powiadamia ADO przekazując *Protokół zagrożenia* (**Załącznik nr 12 do PBI**).
6	Próba kradzieży danych osobowych w formie papierowej	Należy nie dopuścić do kradzieży danych osobowych i powiadomić IOD poprzez Dział Ogólno-Administracyjny. Dział Ogólno-Administracyjny powinien zabezpieczyć dane. IOD powiadamia ADO przekazując *Protokół zagrożenia*.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD poprzez Dział Ogólno-Administracyjny. IOD powiadamia ADO przekazując *Protokół uchybienia*.
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Należy powiadomić IOD poprzez Dział Ogólno-Administracyjny, który powinien zabezpieczyć pomieszczenie. IOD powiadamia ADO przekazując *Protokół uchybienia*.
9	Próba włamania do pomieszczenia/budynku	Należy zabezpieczyć dowody i powiadomić IOD poprzez Dział Ogólno-Administracyjny. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD powiadamia ADO przekazując *Protokół zagrożenia*.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy zawiadomić ASI. ASI przeprowadza audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych i firewall. ASI przekazuje wynik audytu IOD, który powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić *Protokół uchybienia* lub *Protokół zagrożenia*. IOD powiadamia ADO przekazując sporządzony protokół.
11	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić ASI. ASI powinien zaktualizować lub wnioskować o zakup oprogramowania antywirusowego oraz powiadomić IOD poprzez Dział Ogólno-Administracyjny. IOD powiadamia ADO przekazując *Protokół uchybienia*.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Należy zabezpieczyć dowody i powiadomić IOD poprzez Dział Ogólno-Administracyjny. IOD sprawdza stan uszkodzeń, zabezpiecza dowody. IOD powiadamia ADO przekazując *Protokół zagrożenia*.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym	Należy zabezpieczyć dowody i powiadomić ASI/MSI. ASI/MSI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia IOD poprzez Dział Ogólno-Administracyjny. IOD powiadamia ADO

		przekazując *Protokół zagrożenia*.
14	Uszkodzenie komputerów, nośników danych	Należy powiadomić ASI. ASI powinien poprzez Dział Ogólno-Administracyjny powiadomić IOD, który powinien ocenić przyczyny uszkodzenia komputerów, nośników danych. ASI jest odpowiedzialny za ewentualne przywrócenie danych z kopii zapasowej. IOD powiadamia ADO przekazując *Protokół zagrożenia*.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI. ASI powinien poprzez Dział Ogólno-Administracyjny powiadomić IOD. IOD powiadamia ADO przekazując *Protokół uchybienia*.
16	Zdarzenia losowe	IOD we współpracy z ASI/MSI oraz Działem Ogólno-Administracyjnym inwentaryzuje i szacuje straty. IOD powiadamia ADO przekazując *Protokół zagrożenia* lub *Protokół uchybienia*.
17	Dokumentacja niszczona bez użycia niszczarki	Należy zabezpieczyć dane osobowe oraz powiadomić IOD poprzez Dział Ogólno-Administracyjny, który powiadamia ADO przekazując *Protokół uchybienia* (**Załącznik nr 11 do PBI**).
18	Hasła do systemów przechowywane w pobliżu komputera	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI. ASI powinien poprzez Dział Ogólno-Administracyjny powiadomić IOD. IOD powiadamia ADO przekazując *Protokół uchybienia*.
19	Utrata kontroli nad kopią danych osobowych	Podjąć próbę odzyskania kopii. Należy powiadomić IOD poprzez Dział Ogólno-Administracyjny, który we współpracy z ASI/MSI powinien sprawdzić system uwierzytelniania oraz czy nie doszło do kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI/MSI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
20	Kradzież komputerów lub twardych dysków z danymi osobowymi	Należy zabezpieczyć dowody i powiadomić IOD poprzez Dział Ogólno-Administracyjny. IOD inwentaryzuje i szacuje straty, zabezpiecza dowody i wzywa policję. IOD powiadamia ADO przekazując *Protokół zagrożenia*.
21	e-maile zachęcające do ujawnienia identyfikatora i/lub hasła	Należy nie dopuścić do kradzieży danych osobowych i powiadomić IOD poprzez Dział Ogólno-Administracyjny. Dział Ogólno-Administracyjny powinien zabezpieczyć dane. IOD powiadamia ADO przekazując *Protokół zagrożenia*.
22	Telefoniczna próba wyłudzenia danych osobowych	Natychmiast przerwać rozmowę prowadzącą do ujawnienia Informacji. Bezzwłocznie poprzez Dział Ogólno-Administracyjny powiadomić IOD. IOD powiadamia ADO przekazując *Protokół uchybienia*.
23	Ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń.
24	Przesłanie niezaszyfrowanych danych osobowych przez	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Bezzwłocznie poprzez Dział Ogólno-

	Internet	Administracyjny powiadomić IOD. IOD powiadamia ADO przekazując *Protokół uchybienia*.
25	Wpuszczenie do pomieszczeń osób nieznanych i dopuszczenie ich do kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniu do ich opuszczenia, próbować ustalić ich tożsamość. Należy powiadomić IOD poprzez Dział Ogólno-Administracyjny, który we współpracy z ASI/MSI powinien sprawdzić system uwierzytelniania oraz czy nie doszło do kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI/MSI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
26	Dopuszczanie, aby osoby spoza działu DI podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania, próbować ustalić ich tożsamość. Należy powiadomić IOD poprzez Dział Ogólno-Administracyjny, który we współpracy z ASI/MSI powinien sprawdzić czy nie doszło do naruszenia zabezpieczeń, kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI/MSI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
27	Dopuszczenie lub ignorowanie faktu, że osoby spoza działu DI dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania, próbować ustalić ich tożsamość. Należy powiadomić IOD poprzez Dział Ogólno-Administracyjny, który we współpracy z ASI/MSI powinien sprawdzić czy nie doszło do naruszenia zabezpieczeń, kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI/MSI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
28	Dopuszczanie do znalezienia się w pomieszczeniach serwerowni osób spoza działu DI bez bezpośredniego nadzoru pracownika działu DI.	Wezwać osoby bezprawnie przebywające w pomieszczeniu do ich opuszczenia, próbować ustalić ich tożsamość. Należy powiadomić IOD poprzez Dział Ogólno-Administracyjny, który we współpracy z ASI/MSI powinien sprawdzić system uwierzytelniania oraz czy nie doszło do kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI/MSI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
29	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Należy bezzwłocznie zawiadomić ASI. ASI powinien sprawdzić czy nie doszło do naruszenia zabezpieczeń, kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
30	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Należy bezzwłocznie zawiadomić ASI. ASI powinien sprawdzić czy nie doszło do naruszenia zabezpieczeń, kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
31	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Należy bezzwłocznie zawiadomić ASI. ASI powinien sprawdzić czy nie doszło do naruszenia zabezpieczeń, kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, IOD powiadamia ADO przekazując *Protokół uchybienia*.

32	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Należy bezzwłocznie zawiadomić ASI. ASI powinien sprawdzić czy nie doszło do naruszenia zabezpieczeń, kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, IOD powiadamia ADO przekazując *Protokół uchybienia*.
33	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Należy bezzwłocznie zawiadomić ASI. ASI powinien sprawdzić czy nie doszło do naruszenia zabezpieczeń, kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, IOD powiadamia ADO przekazując *Protokół uchybienia*.

§ 42.

1. W przypadku stwierdzenia wystąpienia zagrożenia, IOD we współpracy z Działem Ogólno-Administracyjnym oraz w przypadku wystąpienia zagrożenia w systemach informatycznych ASI/MSI, prowadzi postępowanie wyjaśniające, w toku którego:
   1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
   2) inicjuje ewentualne działania dyscyplinarne;
   3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
   4) dokumentuje prowadzone postępowania.
2. W przypadku stwierdzenia incydentu (naruszenia) IOD prowadzi postępowanie wyjaśniające, w toku którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
   2) ustala osoby odpowiedzialne za naruszenie;
   3) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
   4) dokumentuje prowadzone postępowania.
3. IOD jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. W przypadku stwierdzenia konieczności podjęcia działań korygujących lub zapobiegawczych, określa źródło powstania incydentu, zagrożenia lub słabości, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną.
4. IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

Rozdział 6.
Postanowienia końcowe

§ 43.

1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy RODO.

2. Nad aktualnością Polityki Bezpieczeństwa Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu czuwa IOD we współpracy z Działem Ogólno-Administracyjnym, ASI i MSI.

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ INFORMACJE, W TYM DANE OSOBOWE

Wykaz dotyczy pomieszczeń zlokalizowanych w budynku: ul. Tadeusza Kościuszki 131 50-440 Wrocław

L.p.	Numer pomieszczenia lub określenie jego położenia	Typ strefy	Komórka organizacyjna użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

Załącznik Nr 2
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Lp.	Zbiór danych	Podstawa przetwarzania	Rodzaj systemu przetwarzania danych osobowych	Nazwa systemu informatycznego
1.				
2.				
3.				
4.				
5.				
6.				
7.				

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

Wrocław, dnia ……..

UPOWAŻNIENIE
DO PRZETWARZANIA INFORMACJI, W TYM DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....
zatrudnioną/-ego w Powiatowym Zakładzie Katastralnym we Wrocławiu
na stanowisku .....,
do dostępu i przetwarzania informacji, w tym następujących zbiorów danych osobowych:

1) ……
2) ……
3) ……
4) ……

2. Okres trwania upoważnienia: .....

3. Osoba upoważniona do przetwarzania informacji, w tym danych objętych zakresem zbiorów, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

……..……..

podpis Administratora Danych Osobowych

Data i podpis osoby upoważnionej: .....

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Zobowiązuję się do zachowania w tajemnicy informacji, w tym danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności w Powiatowym Zakładzie Katastralnym we Wrocławiu.

Zobowiązuję się przestrzegać przepisów dotyczących informacji, w tym ochrony danych osobowych określonych w *Polityce Bezpieczeństwa Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu* oraz *Systemie Zarządzania Bezpieczeństwem Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu*.

Oświadczam, że zapoznałem/-am się z *Polityką Bezpieczeństwa Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu* oraz *Systemem Zarządzania Bezpieczeństwem Informacji w Powiatowym Zakładzie Katastralnym we Wrocławiu*, a także znane mi są przepisy art. 107 *ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781)* dotyczące odpowiedzialności karnej za nieprzestrzeganie zasad ochrony danych osobowych.

.....

(data i podpis osoby oświadczającej)

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

Wrocław, dnia ……

UPOWAŻNIENIE
INSPEKTORA OCHRONY DANYCH

Na podstawie art. 37 i następnych Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (RODO)(Dz. Urz. UE L119 z 4 maja 2016 r.)

z dniem ……

powołuję

INSPEKTORA OCHRONY DANYCH

i powierzam tę funkcję Panu/Pani.....

Do obowiązków **Inspektora Ochrony Danych** należy realizowanie zadań wynikających z art. 39 RODO oraz innych powierzonych przez Dyrektora Powiatowego Zakładu Katastralnego we Wrocławiu reprezentującego Administratora Danych Osobowych - Powiatowy Zakład Katastralny we Wrocławiu, w szczególności:

1) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
2) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym lub zabraniem przez osobę nieuprawnioną;
3) zabezpieczenie danych przed ich przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
4) prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne służące ich zabezpieczeniu;
5) zapewnianie przestrzegania przepisów o ochronie danych osobowych poprzez:
    a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (czynności kontrolne),
    b) opracowywanie planów czynności kontrolnych określających przedmiot, zakres, termin poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania,
    c) opracowywanie sprawozdań z czynności kontrolnych,
    d) nadzorowanie opracowania i aktualizowania dokumentacji opisującej środki przetwarzania danych oraz przestrzegania zasad w niej określonych,
    e) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
6) prowadzenie rejestru zbiorów danych przetwarzanych przez ADO.

……

podpis Administratora Danych Osobowych

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Inspektora Ochrony Danych w oparciu o Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (RODO)(Dz. Urz. UE L119 z 4 maja 2016 r.), ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781), rozporządzenia wykonawcze wydane na podstawie przywołanej ustawy oraz przepisy wewnętrzne obowiązujące w Powiatowym Zakładzie Katastralnym we Wrocławiu.

.....

podpis osoby powoływanej na Inspektora Ochrony Danych

Załącznik nr 6
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Komórka organizacyjna	Zbiory danych, do których osoba upoważniona posiada dostęp	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/-y w systemach informatycznych
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Załącznik nr 7
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

L.p.	**Imię i Nazwisko/Nazwa zbioru** *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	**Data udostępnienia**	**Nazwa podmiotu, któremu udostępniono dane** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	**Cel udostępnienia** *(podstawa prawna/numer umowy)*	**Zakres udostępnionych danych** *(jakie dane zostały udostępnione)*	**Rodzaj zbioru/zasobu i jego lokalizacja** *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

WYKAZ PODMIOTÓW, KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

L.p.	Nazwa podmiotu, któremu powierzono dane	Numer umowy i data powierzenia	Cel powierzenia	Zakres powierzonych zbiorów danych	Określenie zbioru/zasobu
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					

Załącznik nr 9
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH OSOBOM KTÓRYCH DOTYCZĄ

L.p.	**Imię i nazwisko osoby, której dane są udostępniane**	**Data udostępnienia**	**Rodzaj zbioru danych/zasobu i jego lokalizacja** *(np. papierowy wydruk danych zawartych w określonym zbiorze)*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

Załącznik nr 10
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

REJESTR INCYDENTÓW I ZAGROŻEŃ DANYCH OSOBOWYCH

L.p.	**Kod**	**Data i godzina incydentu**	**Rodzaj incydentu** *(uchybienie / zagrożenie)*	**Skutki incydentu**	**Działania naprawcze**	**Podpis IOD**
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Załącznik nr 11
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

PROTOKÓŁ UCHYBIENIA

Data i godzina wystąpienia uchybienia ……..

Kod uchybienia ……..

Opis uchybienia:

……

……

……

Przyczyny powstania uchybienia:

……

……

……

Zaistniałe skutki uchybienia:

……

……

……

Podjęte działania naprawczo-zapobiegawcze:

……

……

……

…….. ……..

podpis Inspektora Danych Osobowych *podpis Administratora Danych Osobowych*

Załącznik nr 12
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

PROTOKÓŁ ZAGROŻENIA

Data i godzina wystąpienia zagrożenia ……..……..

Kod zagrożenia ……..

Opis zagrożenia:

……

……

……

Przyczyny powstania zagrożenia:

……

……

……

Zaistniałe skutki zagrożenia:

……

……

……

Podjęte działania naprawczo-zapobiegawcze:

……

……

……

…….. ……..

podpis Inspektora Danych Osobowych *podpis Administratora Danych Osobowych*

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia . . . . . pomiędzy:

. . . . . .

(dane podmiotu, który Umowę zawiera)

zwany w dalszej części Umowy **„Podmiotem przetwarzającym”**

reprezentowany przez:

. . . . . .

oraz

Powiatowym Zakładem Katastralnym we Wrocławiu

ul. T. Kościuszki 131, 40-440 Wrocław

NIP: 8971729038; REGON: 020530640

zwany w dalszej części Umowy ”Administratorem danych osobowych” lub „Administratorem”

reprezentowany przez:

. . . . . – Dyrektora

o następującej treści:

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych osobowych Podmiotowi przetwarzającemu dane osobowe do przetwarzania, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE. L Nr 119, str. 1) (zwanego w dalszej części Umowy „Rozporządzeniem”), na zasadach, w zakresie i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

§ 2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy zbiory danych osobowych . . . . . (**należy podać nazwę zbioru danych)*

2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu …….. (**należy podać cel przetwarzania danych przez podmiot przetwarzający).*
3. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie – które są w minimalnym zakresie niezbędne do realizacji celu o którym mowa w ust. 2 powyżej.

§ 3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z RODO, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane osobowe, przy czym będą to jedynie osoby, które posiadają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do w realizacji celu niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić, że osoby, które upoważnia do przetwarzania danych osobowych, w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w art. 28 ust. 3 pkt b) Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby o których mowa w niniejszym ustępie będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie *usuwa/zwraca* Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. W razie wpływu do Podmiotu przetwarzającego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane, Podmiot przetwarzający niezwłocznie informuje o tym Administratora. Udzielając informacji,

Podmiot przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia.

§ 4
Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 pkt h Rozporządzenia ma prawo kontroli, mającej na celu weryfikację czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego, z minimum 3 dniowym uprzedzeniem o podjęciu działań kontrolnych u Podmiotu przetwarzającego.
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli oraz przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli, w terminie wskazanym przez Administratora nie dłuższym niż 5 dni roboczych. Administrator ustali termin usunięcia uchybień po zrealizowaniu kontroli, na podstawie wniosków pokontrolnych.

§ 5
Raportowanie

1. Na wniosek Administratora, Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z RODO.
2. Informacji, o których mowa w ust. 1, udziela się w terminie 10 dni roboczych od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 24 godzin od doręczenia wniosku.

§ 6
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy z obowiązków wynikających z niniejszej Umowy.

§ 7

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§ 8

Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od …. do …. .*
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem …… dniowego okresu wypowiedzenia.

§ 9

Rozwiązanie Umowy

Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

b) przetwarza dane osobowe w sposób niezgodny z Umową;

c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 10

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§ 11

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla Administratora.

. . . .

Administrator Danych Osobowych Podmiot przetwarzający

Załącznik nr 14
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

REJESTR PRZETWARZANIA ZBIORÓW DANYCH OSOBOWYCH

L.p.	Nazwa zbioru	Podmiot, któremu powierzono przetwarzanie danych	Podstawa prawna przetwarzania danych osobowych	Cel i zakres przetwarzania danych osobowych	Cel przetwarzania danych osobowych	Okres przetwarzania danych osobowych
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Załącznik Nr 15
do Polityki Bezpieczeństwa Informacji
w Powiatowym Zakładzie Katastralnym we Wrocławiu

ARKUSZ ZARZĄDZANIA RYZYKIEM

……., dnia …….

Nazwa komórki organizacyjnej ……

Właściciel ryzyka ……

Lp	*Ryzyko*	*Prawdopodobieństwo* wystąpienia ryzyka (skala 1-4 pkt)*	*Skutek** (skala 1-4 pkt)*	*Poziom wpływu ryzyka na bezpieczeństwo (Istotność ryzyka)*** (skala 1-16 pkt)*	*Ocena ryzyka – wynik (dopuszczalność)*	*Istniejące mechanizmy kontroli*	*Propozycje reakcji na ryzyko*	*Uwagi*

……

Kierownik komórki organizacyjnej

……

Inspektor Ochrony Danych

……

Administratoa Danych Osobowych

LEGENDA

* Sposób oceny prawdopodobieństwa wystąpienia ryzyka

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
Bardzo wysokie (81-100%)	**4**	Przewiduje się, że zdarzenie z pewnością wystąpi w ciągu roku
Wysokie (61-80%)	**3**	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku
Średnie (21-60%)	**2**	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub kilka razy w ciągu roku
Niskie (0-20%)	**1**	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku

** Sposób oceny skutku ryzyka

Skutek wystąpienia ryzyka*	Ilość punktów	Przesłanki
Bardzo wysoki	4	Poważna niezgodność z przepisami prawa. Brak procedur dla danego procesu. Olbrzymie zakłócenia pracy. Znaczny uszczerbek na wizerunku. Zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Brak osiągnięcia kluczowych celów. Straty finansowe.
Wysoki	3	Duże zagrożenie realizacji kluczowych zadań albo osiągania założonych celów. Dotkliwa strata finansowa. Znaczny uszczerbek na wizerunku. Długotrwały i trudny proces przywracania stanu poprzedniego.
Średni	2	Spadek efektywności działania i obniżenie jakości wykonywania zadań. Niewielka strata finansowa. Nieznaczny negatywny wpływ na wizerunek. Trudny proces przywracania stanu poprzedniego
Niski	1	Zakłócenie lub opóźnienie w wykonywaniu zadań. Bez uszczerbku dla wizerunku. Skutki łatwe do usunięcia

***Skala dopuszczalności ryzyka:

Oszacowanie ryzyka	Dopuszczalność ryzyka	Działania
Ryzyko poważne Skala: 13 - 16 pkt.	Niedopuszczalne (nieakceptowane)	Działania nie mogą być podjęte ani kontynuowane do czasu zmniejszenia ryzyka do poziomu dopuszczalnego
Ryzyko wysokie Skala: 9 – 12 pkt.	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań ,których celem jest zdecydowane zmniejszenie ryzyka
Ryzyko umiarkowane Skala: 5 - 8 pkt	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań ,których celem jest zdecydowane i skuteczne zmniejszenie ryzyka
Ryzyko nieznaczne Skala: 1- 4 pkt	Dopuszczalne (akceptowane)	Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie

LISTA MECHANIZMÓW KONTROLI REDUKUJĄCYCH RYZYKO

1. Regulacje zewnętrzne i wewnętrzne,
2. Opis funkcji i stanowisk, zakresy czynności i obowiązków.
3. System obiegu informacji i raportowania.
4. Uzgadnianie stanowisk, kierunków działań.
5. Uzgadnianie danych, tzw. rekonsyliacja,
6. Zasada komisyjności „czworga oczu", „na dwie ręce" (wykonywanie czynności przy współudziale co najmniej dwóch osób, komisje inwentaryzacyjne, spisowe, zespoły kontrolne, rejestracja i autoryzacja dowodów księgowych lub transakcji),
7. System limitów i ograniczeń,
8. Analiza kontrahentów/uczestników rynku,
9. Kontrola dostępu oraz zabezpieczenia teleinformatyczne (zakazy i ograniczenia dostępu fizycznego osób do pomieszczeń, systemów i danych, Internetu, zagranicznych rozmów telefonicznych, możliwości nagrywania rozmów telefonicznych),
10. Inwentaryzacja i spis z natury,
11. Zabezpieczenia fizyczne,
12. Kopie zapasowe, na wypadek utraty oryginalnych danych, zapasowe generatory prądotwórcze, na wypadek awarii zasilania,
13. Plany zarządzania kryzysem,
14. Rezerwy finansowe, na pokrycie strat związanych np. z niewypłacalnością kontrahentów, koniecznością pokrycia strat,
15. Ubezpieczenia mienia od zdarzeń losowych, kradzieży, itp.,
16. Usługi zewnętrzne, dzielenie się ryzykiem, które obciążałoby jednostkę w sytuacji gdyby zadania były wykonywane przy wykorzystaniu zasobów własnych,
17. Audyt - kontrola bieżąca i następcza,
18. Analiza mierników,
19. Testowanie nowych rozwiązań, projektów, systemów informatycznych przed ich wdrożeniem,
20. Zarządzanie bezpieczeństwem informacji, szkolenie pracowników,
21. Analiza informacji przekazywanych od pracowników oraz pozyskiwanych od stron zewnętrznych.