ZARZĄDZENIE NR 701./16
B U R M I S T R Z A Ś W I E C I A
z dnia 16 grudnia 2016 roku.

w sprawie wdrożenia Polityki Bezpieczeństwa Informacji Urzędu Miejskiego w Świeciu.

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. 2016, poz. 922), § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 r. Nr 100, poz. 1024),

zarządzam co następuje:

§ 1. Wprowadzić Politykę Bezpieczeństwa Informacji Urzędu Miejskiego w Świeciu, której treść stanowi ***załącznik*** do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 3. Traci moc Zarządzenie Nr 1298/10 Burmistrza Świecia z dnia 1 marca 2010 roku w sprawie organizacji i dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
TADEUSZ POGODA

POLITYKA BEZPIECZEŃSTWA INFORMACJI

URZĘDU MIEJSKIEGO W ŚWIECIU

Niniejszy dokument jest sporządzony na podstawie Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz Polską Normą PN – ISO / IEC 27001:2014 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania.

1. Informacje wstępne

Polityka Bezpieczeństwa Informacji zwana dalej „Polityką" jest dokumentem wewnętrznym **Urzędu Miejskiego w Świeciu** i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

Każda osoba mająca dostęp do informacji zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

2. Misja jednostki

Misją jednostki jest realizacja zadań publicznych, wynikających z przepisów ustaw oraz aktów wykonawczych. Nadto, zadaniem podmiotu jest budowanie wizerunku nowoczesnej administracji publicznej poprzez skuteczną i zgodną z przepisami prawa obsługę interesantów w sposób: profesjonalny, nowoczesny i przyjazny, przy jednoczesnym dążeniu do zapewnienia wysokiej jakości obsługi.

3. Cel wdrożenia Polityki Bezpieczeństwa Informacji

Celem opracowania i wdrożenia Polityki Bezpieczeństwa Informacji jest zdefiniowanie ogólnych wymagań i zasad ochrony informacji, które będą fundamentem dla wszystkich dokumentów związanych z bezpieczeństwem informacji.

4. Deklaracja stosowania

Mając na uwadze misje oraz cele jednostki Administrator Danych Osobowych ustanawia Politykę Bezpieczeństwa Informacji oraz deklaruje:

a) podejmowanie wszystkich działań niezbędnych dla zapewnienia legalności przetwarzanych danych,

b) stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane w zakresie problematyki bezpieczeństwa tychże danych,

c) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym

danym,

d) dążenie do zapewnienia poufności, dostępności oraz integralności informacji chronionych w tym szczególnie danych osobowych.

5. Kontekst zewnętrzny

Gmina Świecie jest gminą miejsko-wiejska w województwie kujawsko-pomorskim, w powiecie świeckim. W skład gminy wchodzi 13 sołectw. Gmina Świecie sąsiaduje z następującymi gminami: Bukowiec, Chełmno, Chełmno, Dragacz, Drzycim, Jeżewo, Pruszcz. Siedzibą Gminy jest miejscowość Świecie.

6. Podstawa prawna

Polityka bezpieczeństwa informacji oraz inne dokumenty szczegółowe związane z bezpieczeństwem informacji opierają się na:

1) Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 r. poz. 922 z późn.zm.);
2) Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2014 r. poz. 1114 z późn.zm.);
3) Ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2015 r. poz. 2058 z późn.zm.);
4) Ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. 2003 r. Nr153, poz. 1503 z późn.zm.);
5) Rozporządzeniu 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. 2016 r. poz. 113 z późn.zm.);
6) Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr100, poz. 1024 z późn.zm.);

7) Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004r. w sprawie wzoru imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. 2004 r. Nr94, poz. 923 z późn.zm.);
8) Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. 2008 r. Nr229, poz. 1536 z późn.zm.);
9) Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014 r. poz. 1943 z późn.zm.);
10) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015r. poz. 719, z późn.zm.);
11) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015 r. poz. 745 z późn.zm.);
12) Polskiej Normie PN-ISO/IEC 27001:2014;
13) Polskiej Normie PN-ISO/IEC 27005:2014.

7. Definicje

1) **Administrator Danych** - Gmina Świecie, reprezentowana przez Burmistrza;

Administrator Danych Osobowych w myśl ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;

2) **Administrator Bezpieczeństwa Informacji /ABI/** - osoba, powołana i zgłoszona przez Administratora Danych do rejestracji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych;

3) **Administrator Systemu Informatycznego /ASI/** - osoba zarządzająca systemem informatycznym, w którym przetwarzane są dane osobowe;

4) **Analiza ryzyka** - proces dążący do poznania charakteru *ryzyka* oraz określenia *poziomu ryzyka*;

5) **Audyt** - systematyczny, niezależny i udokumentowany *proces* uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu;

6) **Bezpieczeństwo informacji** - zachowanie *poufności*, *integralności* i *dostępności* informacji;

7) **Dostępność** - właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu;

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

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

10) **Identyfikowanie ryzyka** - proces wyszukiwania, rozpoznawania i opisywania *ryzyka*;

11) **Informacje/dane chronione:**

Dane osobowe wg ustawy z dnia 29 sierpnia 1997 r. „za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej",

Tajemnice przedsiębiorstw zgodnie z ustawą o zwalczaniu nieuczciwej konkurencji rozumie się „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne, przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności",

Dokumenty oraz informacje w nich zawarte, do których Administrator Danych podpisał umowy o zachowaniu ich w poufności;

12) **Integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

13) **Incydenty związane z bezpieczeństwem informacji** - pojedyncze niepożądane lub niespodziewane *zdarzenie związane z bezpieczeństwem informacji* lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają *bezpieczeństwu informacji*;

14) **Integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności;

15) **Odbiorca danych** - każdy, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,

d) podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

16) **Osoba upoważniona do przetwarzania danych osobowych** - osoba, upoważniona do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie;

17) **Polityka** - zamierzenia i kierunki organizacji formalnie wyrażone przez jego *najwyższe kierownictwo*;

18) **Pomieszczenia** - budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w formie dokumentacji papierowej;

19) **Podatność** - słabość aktywu lub *zabezpieczenia*, która może być wykorzystana przez co najmniej jedno *zagrożenie*;

20) **Poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;

21) **Postępowanie z ryzkiem** - *proces* modyfikowania *ryzyka*;

22) **Prawdopodobieństwo** - możliwość wystąpienia zdarzenia;

23) **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

24) **Przetwarzający** - podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy o ochronie danych osobowych;

25) **Raport** - przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

26) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

27) **Sieć publiczna** - sieć telekomunikacyjna niebędącą siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych;

28) **Sieć telekomunikacyjna** - urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną;

29) **Serwisant** - firma lub pracownik firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

30) **System informatyczny** - sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; system ten tworzy sieć teleinformatyczną Administratora Danych;

31) **Teletransmisja** - przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

32) **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

33) **Użytkownik** - osoba upoważniona do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

34) **Zabezpieczenie** - środek, który modyfikuje *ryzyko*;

35) **Zagrożenie** - potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji;

36) **Zarządzanie incydentami związanymi z bezpieczeństwem informacji** - procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji;

37) **Zarządzanie ryzykiem** - skoordynowane działania dotyczące kierowania i nadzorowania *organizacji* w odniesieniu do *ryzyka*;

38) **Zbiór danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

8. Oznaczenie informacji

Osoby posiadające upoważnienia (pisemne lub ustne) oraz mające dostęp do informacji w związku z zajmowanym stanowiskiem lub pełnioną funkcją, samodzielnie klasyfikują informacje, a w przypadku informacji chronionej mają obowiązek stosować zapisy niemniejszego dokumentu.

9. Polityka przetwarzania danych

Osoby odpowiedzialne za bezpieczeństwo informacji i przetwarzanie danych osobowych

Administrator Danych /AD/

Administrator danych realizuje zadania w zakresie ochrony informacji chronionych, w tym zwłaszcza:

a) dąży do zapewnienia poufności, integralności i dostępności informacji chronionych;

b) podejmuje decyzje o celach i środkach przetwarzania danych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji Administratora Danych oraz technik zabezpieczenia danych;

c) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;

d) odwołuje upoważnienia do przetwarzania danych osobowych;

e) może powołać Administratora Bezpieczeństwa Informacji (art. 36a ust.1); Administrator Danych Osobowych w przypadku powołania Administratora Bezpieczeństwa Informacji obowiązany jest zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie Administratora Bezpieczeństwa Informacji w terminie 30 od dnia jego powołania/odwołania;

f) wyznacza Administratora Systemu Informatycznego oraz określa zakres jego zadań i czynności;

g) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania informacji chronionej niekiedy innych danych osobowych;

h) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji /ABI/

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za prowadzenie całokształtu spraw związanych przetwarzaniem danych chronionych, a w szczególności za:

a) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (**oświadczenie o znajomości Polityki załącznik nr 4**);
b) aktualizacja dokumentacji z ochrony informacji tj. Polityki bezpieczeństwa informacji;
c) prowadzenie szkoleń uświadamiających z zakresu bezpieczeństwa informacyjnego dla nowozatrudnionych pracowników oraz szkoleń okresowych dla pozostałych pracowników;
d) przygotowywanie upoważnień dla pracowników;
e) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowy;
f) inicjowanie okresowej analizy ryzyka;
g) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;
h) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 u.o.d.o.;
i) zgłaszanie do rejestru GIODO zbiorów z danymi wrażliwymi;
j) przygotowywanie projektów lub opiniowanie projektów umów powierzenia przetwarzania danych osobowych.

Administrator Systemu Informatycznego /ASI/

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych, w tym zwłaszcza:

a) zarządza systemem informatycznym, w którym przetwarzane są informacje chronione, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
b) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego,

w którym przetwarzane są informacje chronione;

c) przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym;

d) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych;

e) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;

f) wyrejestrowuje użytkowników;

g) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby Administratorowi Bezpieczeństwa Informacji lub Administratorowi Danych;

h) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora Bezpieczeństwa Informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;

i) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych chronionych przetwarzanych w systemie informatycznym;

j) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane chronione, nad wykonywaniem kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;

k) prowadzi rejestr wykonywanych kopii zabezpieczających oraz dziennik systemu informatycznego;

l) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;

m) prowadzi inwentaryzację sprzętu komputerowego i oprogramowania.

Rejestr zbiorów danych osobowych

1) rejestr zbiorów danych składa się z wykazu zbiorów danych osobowych przetwarzanych w jednostce, zawierającego odrębnie dla każdego zbioru danych informacje;
2) rejestr prowadzony jest w postaci elektronicznej i papierowej;
3) za prowadzenie rejestru zgodnie z obowiązującymi przepisami i jego aktualizację odpowiada powołany przez Administratora Danych Osobowych - Administrator Bezpieczeństwa Informacji;
4) Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru dokonuje:
   a. wpisania zbioru danych w przypadku rozpoczęcia przetwarzania w nim danych osobowych,
   b. aktualizacji informacji dotyczących zbioru danych w przypadku zmiany informacji objętych wpisem,
   c. wykreślenia zbioru danych, w przypadku zaprzestania przetwarzania w nim danych osobowych;
5) wpisu do rejestru dokonuje się niezwłocznie po zaistnieniu zdarzenia, o którym mowa w pkt 4 pkt a powodującego obowiązek dokonania wpisu;
6) w rejestrze prowadzi się wykaz zmian, który zawiera:
   a. wskazanie rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie),
   b. datę dokonania zmiany,
   c. zakres zmiany.

Upoważnienia do przetwarzania danych osobowych

1) Każdy pracownik przetwarzający dane osobowe powinien zostać upoważniony na piśmie do ich przetwarzania przez Administratora Danych Osobowych, zgodnie z art. 37 uodo. Wzór upoważnienia stanowi **załącznik nr 5** do niniejszej Polityki.
2) W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, przyjęcia do pracy nowego pracownika lub stażysty, lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, Administrator Danych Osobowych zobowiązany jest wydać nowe lub cofnąć upoważnienie.

3) Administrator Danych Osobowych nadaje upoważnienia na czas określony lub nieokreślony.

Ewidencja osób upoważnionych

Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji i zawiera w szczególności:

a) imię i nazwisko osoby upoważnionej,

b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

c) identyfikator, jeżeli dane przetwarzane są w systemie informatycznym.

Ewidencja stanowi **załącznik nr 6.**

Infrastruktura przetwarzania danych chronionych

Wykaz budynków i pomieszczeń tworzących obszar przetwarzania danych osobowych - **załącznik nr 1,**

Wykaz i struktura zbiorów danych osobowych - **załącznik nr 2,**

Sposób przepływu danych pomiędzy systemami informatycznymi - **załącznik nr 3.**

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

Polityka kluczy

Budynek Urzędu Miejskiego w Świeciu podlega ochronie polegającej na całodobowym monitorowaniu przez system alarmowy zainstalowany w budynku.

W godzinach pracy, zobowiązuję się pracowników do:

a) zwracania szczególnej uwagi na zachowanie osób wchodzących i wychodzących z siedziby jednostki;

b) reagowania na wejście do budynku i przebywanie w nim osób będących pod wpływem alkoholu lub innych środków odurzających;

c) reagowania na próby niszczenia, wynoszenia lub wywożenia mienia z budynku jednostki;

d) reagowania na próby wnoszenia do budynku przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie itp.;

e) natychmiastowego reagowania poprzez powiadomienie odpowiednich służb (Straż Miejska, Policja, Straż Pożarna, Pogotowie Ratunkowe) o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.

Administrator Danych wyznacza pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy jednostki.

Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do :

a) wykorzystywania ich zgodnie z przeznaczeniem,

b) nie kopiowania powierzonych kluczy bez zgody Administratora Danych oraz udostępniania osobom trzecim,

c) nie udostępniania kodu cyfrowego do systemu alarmowego osobom trzecim.

Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia.

W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń, o których mowa powyżej, pracownik, który to stwierdził, natychmiast powiadamia o tym swojego bezpośredniego przełożonego.

Od momentu pobrania kluczy do momentu ich zdania na pracownikach urzędujących w tych pomieszczeniach spoczywa pełna odpowiedzialność za ich zabezpieczenie.

Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających na:

a) zabezpieczeniu dokumentacji i pieczęci urzędowych;

b) zabezpieczeniu komputerów i nośników informacji;

c) wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;

d) zamknięciu okien i drzwi;

e) pozostawieniu kluczy od pomieszczeń biurowych w sekretariacie.

Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

Do otwierania pomieszczeń dla potrzeb wykonania czynności związanych ze sprzątaniem wykorzystywane są klucze zdane przez pracowników w sekretariacie.

Bezpieczeństwo osobowe

1) Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2) Ryzyko utraty bezpieczeństwa danych przetwarzanych przez Administratora Danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest

minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

3) Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia Administratora Danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie pisemnych oświadczeń.

Zabezpieczenia we własnym zakresie /po stronie personelu/

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie, przez każdą osobę upoważnioną do ich przetwarzania, nawyku: -

a) **polityki „czystego ekranu"** - w przypadku chwilowego opuszczenia stanowiska pracy pracownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych;

b) **polityki „czystego biurka"** - w trakcie pracy pracownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy pracownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych;

c) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);

d) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);

e) pilnego strzeżenia akt, płyt CD/DVD, pamięci przenośnych i komputerów przenośnych;

f) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie w miejscu niezabezpieczonym przed dostępem osób trzecich, a w szczególności w postaci niezaszyfrowanej na komputerach lub nośnikach danych. Hasła nigdy nie zapisujemy w postaci jawnej;

g) powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;

h) udostępnianie danych osobowych pocztą elektroniczną powinno odbywać się tylko w postaci zaszyfrowanej. Hasło do zaszyfrowanej wiadomości przekazujemy drugim kanałem komunikacyjnym np. przez telefon, sms, fax;

i) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

j) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej;

k) zachowania tajemnicy danych, w tym także wobec najbliższych - **oświadczenie o poufności załącznik nr 4**;

l) umieszczania kluczy do szaf w bezpiecznym miejscu po zakończeniu dnia pracy;

m) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

n) zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

Komputery przenośne, na których są przetwarzane dane chronione poza siedzibą urzędu

Przetwarzanie danych chronionych na komputerach przenośnych poza siedzibą Urzędu Miejskiego w Świeciu, powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie za zgodą Administratora Danych.

Każdy komputer przenośny musi być zabezpieczony indywidualnym identyfikatorem i loginem.

Pracownik korzystający z komputera przenośnego do przetwarzania danych chronionych, zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed ich zniszczeniem, utratą i uszkodzeniem.

W związku z powyższym użytkownik komputera przenośnego zobowiązany jest do:

a) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 - znakowym zawierającym: małe, wielkie litery, znaki specjalne lub cyfry,

b) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,

c) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,

d) zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym).

10. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych

Nadawanie uprawnień

1) Administrator Systemu Informatycznego nadaje uprawnienia użytkownikom do pracy w systemach informatycznych na wniosek bezpośredniego przełożonego pracownika/użytkownika - **załącznik nr 7 wzór wniosku.**

2) Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać **wyłącznie osoba upoważniona** do przetwarzania danych osobowych.

3) Dodatkowe uprawnienia mogą zostać przyznane użytkownikowi w przypadku zaistnienia takiej potrzeby. Wówczas użytkownik zobowiązany jest udokumentować i zgłosić taką potrzebę Administratorowi Danych.

4) Administrator Danych podejmuje decyzję czy w danym przypadku zmiana uprawnień jest wskazana.

5) Administrator Systemu Informatycznego dokonuje modyfikacji uprawnień w zależności od rodzaju i zakresu prac.

6) Uprawnienia użytkowników w poszczególnych systemach informatycznych zostały określone w upoważnieniu do przetwarzania danych osobowych.

Wyrejestrowywanie uprawnień

1) Wyrejestrowanie użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego, na wniosek bezpośredniego przełożonego pracownika/użytkownika.
2) Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4) Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 30 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych.
5) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   a) wypowiedzenie umowy o pracę,
   b) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych chronionych.
6) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

Administrator Systemu Informatycznego przeprowadza okresową kontrolę uprawnień i kont użytkowników co najmniej raz na kwartał, w celu weryfikacji czy pracownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych. Z przeprowadzonej kontroli Administrator Systemu Informatycznego sporządza notatkę służbową.

Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

Identyfikator

1) Identyfikator jest dobierany indywidualnie przez ASI. W identyfikatorze pomija się polskie znaki diakrytyczne. W przypadku dublowania się identyfikatorów zostanie on rozszerzony o kolejne litery lub cyfry.
2) W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu Informatycznego, nadaje inny identyfikator, odstępując od zasady określonej w pkt 1.

Polityka haseł

1) Hasło powinno składać się z unikalnego zestawu **co najmniej ośmiu znaków,** zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2) Zmiana hasła do systemu następuje nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3) **Jeśli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik.**
4) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
5) Zabronione jest zapisywanie haseł w sposób jawny.

Hasło administracyjne/najwyższego poziomu

Hasła najwyższego poziomu (administracyjne) do urządzeń i systemów informatycznych winny być przechowywane w miejscu wskazanym przez Administratora Danych. Powyższa ewidencja powinna zawierać nazwę użytkownika (administratora), hasło, sposób dostępu, adres IP serwera urządzenia. Hasła te podlegają zmianie w cyklu półrocznym oraz w sytuacji, gdy dochodzi do zmian personalnych wśród osób, które miały do nich dostęp lub je znały. Powinny cechować się one właściwą złożonością tzn. co najmniej 12 znaków, 3 z 4 grup znaków (małe litery, duże litery, cyfry, znaki specjalne).

Ochrona kluczy kryptograficznych/podpisów elektronicznych

Dokumenty przesyłane drogą elektroniczną, które nie stanowią informacji publicznej powinno zabezpieczać się przy pomocy środków ochrony kryptograficznej. Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków zabezpieczających dane, przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych, gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych danych lub uwierzytelnienie podmiotów lub uwierzytelnienie informacji. Klucze kryptograficzne (hasła, kody, certyfikaty, karty), powinny być zabezpieczone w sposób uniemożliwiający dostęp osobom nieuprawnionym. Rodzaj i model urządzenia kryptograficznego objęty jest zachowaniem poufności w związku z faktem, iż stanowi on element systemu zabezpieczającego.

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

Tryb pracy na poszczególnych stacjach roboczych

1) Rozpoczęcie pracy na stacji roboczej następuje po:
   a) włączeniu napięcia w listwie podtrzymującej napięcie i/lub włączeniu zasilacza awaryjnego (UPS) i komputera,
   b) włączeniu jednostki centralnej stanowiska komputerowego,
   c) włączeniu pozostałych urządzeń peryferyjnych (np. drukarki),
   d) wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora.
2) W pomieszczeniu, w którym przetwarzane są dane, mogą znajdować się osoby postronne w obecności pracownika upoważnionego do przetwarzania danych osobowy.
3) Przed osobami postronnymi, w miarę możliwości, należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
4) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
5) Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami

Administratora Danych a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.

6) Obowiązuje zakaz wynoszenia bez zgody Administratora Danych na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

7) **Zakończenie pracy na stacji roboczej następuje po prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i/lub listwie.**

Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1) Elektroniczne nośniki to: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.

2) Dane osobowe wynoszone poza Urząd muszą być zaszyfrowane.

3) W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.

Kopie zapasowe

Dane, w tym dane osobowe przetwarzane w systemach informatycznych Urzędu, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego.

W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa wybrana kopia powinna być poddawana próbie odtworzeniowej. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość poprawnego odczytania danych. Każdorazowo przeprowadzona próba jest odnotowywana w dzienniku kopii zapasowych.

Powyższe próby powinny być wykonywane nie rzadziej niż raz w miesiącu, a w cyklu kwartalnym powinno się testowo odtworzyć wszystkie kopie zapasowe.

Zasady bezpiecznego użytkowania sprzętu IT

1) Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych, laptopów, serwerów, drukarek, skanerów, smartfonów, pendrive'ów i dysków przenośnych.

2) Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.

3) Użytkownik ma obowiązek natychmiast zgłosić utratę lub zniszczenie powierzonego sprzętu IT.

4) Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączenie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

5) **Pracownicy nie mogą bez zgody Administratora Danych korzystać z prywatnego sprzętu IT (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych.**

Zasady korzystania z oprogramowania

1) Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w jednostce.

2) Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie IT przez Administratora danych na swoje własne potrzeby ani na potrzeby osób trzecich.

3) Instalowanie jakiegokolwiek oprogramowania na sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.

4) Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Administratora Danych Osobowych. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

5) Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.

6) Użytkownicy nie mają prawa posiadania i przechowywania prywatnych filmów, zdjęć itp.

7) W przypadku naruszenia któregokolwiek z powyższych postanowień Administrator Systemu Informatycznego ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

Zasady korzystania z Internetu

1) Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Systemu Informatycznego tylko w uzasadnionych przypadkach.

2) Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu bez zgody osób upoważnionych.

3) Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowania).

4) Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania hasła.

5) W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódki) oraz adresu www rozpoczynającego się frazą „https:" a następnie sprawdzić na jaki podmiot certyfikat został wystawiony.

6) Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności i prawa autorskiego.

7) Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, hasła, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

8) Użytkownicy mogą także korzystać z Internetu dla celów prywatnych, ale wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum.

9) Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych

10) W zakresie dozwolonym przepisami prawa, Administrator Danych Osobowych zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z Internetu pod kątem wyżej

opisanych zasad.

11) Ponadto, w uzasadnionym zakresie, Pracodawca zastrzega sobie prawo do kontroli czasu spędzonego przez użytkownika w Internecie.

12) Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

Zasady korzystania z poczty elektronicznej

1) Przesyłanie danych osobowych z użyciem poczty elektronicznej poza organizację może odbywać się tylko przez osoby do tego upoważnione.

2) W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików).

3) W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery, cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4) Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5) Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6) Nie należy otwierać załączników (plików) w wiadomościach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

7) Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej „łańcuszków szczęścia", itp.

8) Użytkownicy nie powinni rozsyłać maili zawierających załączniki o dużym rozmiarze.

9) Użytkownicy powinni okresowo kasować niepotrzebne wiadomości.

10) Podczas wysyłania korespondencji do wielu adresatów jednocześnie należy użyć metody „Ukryte do wiadomości-UDW".

11) Poczta elektroniczna jest przeznaczona wyłącznie do wykonywania obowiązków służbowych.

12) Użytkownicy mają prawo korzystać z poczty elektronicznej dla celów prywatnych wyłącznie

okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

13) Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

14) Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności i prawa autorskiego.

15) Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

16) Użytkownik bez zgody Administratora Danych nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu.

17) Użytkownicy po wyrażeniu zgody Administratora Danych, mają prawo do korzystania z poczty elektronicznej prywatnej w celach służbowych.

Zasady korzystania z bankowości elektronicznej

1) Użytkownik korzystający z bankowości elektronicznej zobowiązany jest do regularnej zmiany hasła.

2) Użytkownik nie powinien przechowywać hasła razem z loginem wykorzystywanych w bankowości elektronicznej.

3) Użytkownik zalogowany do systemu bankowości elektronicznej nie powinien odchodzić od komputera.

4) Użytkownik powinien niezwłocznie wylogować się i zamknąć przeglądarkę po zakończeniu pracy.

5) Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.

6) Użytkownik w celu zalogowania się do systemu bankowości elektronicznej nie powinien wchodzić

na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.

Sposoby zabezpieczania systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1) Komputery stacjonarne **zabezpieczone są programem antywirusowym,** które sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
2) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych przez Administratora Danych.
3) Obowiązkiem Administratora Systemu Informatycznego jest aktualizacja oprogramowania antywirusowego.
4) Użytkownik jest obowiązany każdorazowo zawiadomić Administratora Systemu Informatycznego o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.
5) Użytkownik zobowiązany jest do postępowania zgodnie z rekomendacjami oprogramowania antywirusowego (np. w kwestii skanowania nowo podpiętych nośników danych).
6) Oprogramowanie antywirusowe jest monitorowane centralnie przez ASI.

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

1) Przeglądu i konserwacji systemu dokonuje Administrator Systemu Informatycznego.
2) Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu Informatycznego dokonuje nie rzadziej niż raz na miesiąc.

Podstawa prawna przetwarzania danych osobowych

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe;
2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa;
3) jest to konieczne dla realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną, lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
4) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora Danych albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności; marketing bezpośredni produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Obowiązek informacyjny przy przetwarzaniu danych

W przypadku zbierania danych od osoby, której dane dotyczą Administrator Danych jest zobowiązany poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem Danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorach lub kategoriach odbiorców danych,

3) prawie dostępu do treści swoich danych oraz ich poprawiania,

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator Danych Osobowych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem Danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,

2) celu i zakresie zbierania danych, a w szczególności o odbiorach lub kategoriach odbiorców danych,

3) źródle danych,

4) prawie dostępu do treści swoich danych oraz ich poprawiania,

5) prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadku gdy, Administrator Danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Wymienionych zasad nie stosuje się, jeżeli:

1) dane są przetwarzane przez administratora na podstawie przepisów prawa,

2) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,

3) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

3) Zapisy logów systemowych powinny być przeglądane przez Administratora Systemu Informatycznego każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

11. Procedura zapewnienia ciągłości działania

Celem procedury jest zminimalizowanie mogących wystąpić nieprawidłowości w funkcjonowaniu Jednostki, spowodowanych dysfunkcją systemu informatycznego. Procedura określa postępowanie w przypadku wystąpienia zdarzeń, mogących wpłynąć na bezpieczeństwo informacji, zarówno realnie jaki i potencjalnie oraz ciągłość działania Urzędu Miejskiego w Świeciu.

O podjęciu działań wskazanych w procedurze decyduje Administrator Danych w porozumieniu Administratorem Bezpieczeństwa Informacji oraz Administratorem Systemu Informatycznego.

Działania zapewniające przywrócenie zdolności realizowania zadań przez Urząd:

1) Sprawdzenie, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.
2) Ustalenie co jest przyczyną awarii:
    a) działanie siły wyższej np. pożar, powódź,
    b) przerwa w zasilaniu,
    c) brak połączenia z siecią,
    d) wadliwe działanie sprzętu,
    e) wadliwe działanie aplikacji,
    f) wadliwe działanie systemu, na którym uruchomiona jest aplikacja.
3) Określenie skali awarii oraz ustalenie czy awaria powoduje zatrzymanie pracy:
    a. jednego pomieszczenia pracy lub wydziału,
    b. całego urzędu.
4) Weryfikacja czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji czy w

lokalizacjach alternatywnych.

5) Zapewnienie/zakupienie niezbędnych elementów wyposażenia, dokonanie naprawy lub wymiany urządzeń, uruchomienie aplikacji.
6) Sprawdzenie czy aplikacja może być uruchomiona, na którymś z działających poprawnie serwerów.
7) W razie potrzeby, uruchomienie serwera zastępczego. W tym celu można wykorzystać np. komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.
8) Usunięcie przyczyny nieprawidłowego działania, a następnie przywrócenie funkcjonowania aplikacji/systemu. W razie konieczności odtworzenie aplikacji z kopii zapasowych.
9) Weryfikacja działania naprawianej aplikacji/systemu.
10) Uruchomienie usługi w systemie informatycznym Urzędu.

12. Aktualizacja regulacji w zakresie zmieniającego się otoczenia

Niniejsza polityka podlega regularnym (nie rzadziej niż raz na rok) przeglądom przez Administratora Bezpieczeństwa Informacji. W zależności od potrzeb mogą zostać przeprowadzone dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Jednostce, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie) Celem przeglądów polityki jest zapewnienie jej stosowalności w stosunku do realizowanych zadań oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian.

13. Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji

Administrator Systemu Informatycznego jest odpowiedzialny prowadzenie inwentaryzacji sprzętu komputerowego i oprogramowania oraz utrzymywanie go w aktualności.

14. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności i poufności informacji

Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenie priorytetów dla zarządzania ryzykami i zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio: unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację.

Analizę ryzyka dokonuje się w oparciu o metody wybrane przez kierownictwo. Zaleca się, by zarządzanie ryzykiem w bezpieczeństwie informacji zapewniało:

a) zidentyfikowanie ryzyka,

b) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia,

c) informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji,

d) ustanowienie priorytetów postępowania z ryzykiem,

e) określenie priorytetów dla działań podjętych w celu zredukowania ryzyka,

f) zaangażowanie uczestników w momencie podejmowania decyzji w procesie zarządzania ryzykiem oraz stałe informowanie ich o statusie zarządzania ryzykiem,

g) skuteczność monitorowania z ryzkiem,

h) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,

i) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem,

j) szkolenie kierownictwa w zakresie ryzyka oraz działań podejmowanych w celu ograniczenia ryzyka.

15. Szkolenia osób zaangażowanych w proces przewarzania informacji

Administrator Bezpieczeństwa Informacji uwzględnia następujący plan szkoleń:

1) niezależnie od zmian prawnych wykonuje szkolenia nie rzadziej niż jeden raz w roku,

2) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych chronionych przeprowadzane są w przypadku każdej istotnej zmiany zasad lub procedur ochrony informacji,
3) nowoprzyjęci pracownicy mają obowiązek samodzielnie zaznajomić się z przepisami prawa w zakresie danych osobowych oraz treścią Polityki bezpieczeństwa informacji. Ich wiedza jest weryfikowana poprzez test wykonany na platformie e-learningowej. Warunkiem zaliczenia jest uzyskanie wyniku na poziomie 80% poprawnych odpowiedzi.

Administrator Danych informuje Administratora Bezpieczeństwa Informacji o konieczności przeprowadzenia szkolenia dla pracowników i stażystów.

Dodatkowo Administrator Bezpieczeństwa Informacji informuje za pomocą poczty elektronicznej o aktualnych zagrożeniach (prowadzi ich monitoring) oraz wysyła planowe wiadomości dotyczące zapisów Polityki bezpieczeństwa informacji celem utrwalenia wiedzy.

Tematyka szkoleń obejmuje następujące zagadnienia:

1) Ochronę danych osobowych według wymogów wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz aktów wykonawaych do ustawy,
2) Bezpieczeństwo systemów informatycznych wg. 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,
3) Dobre praktyki w zakresie bezpieczeństwa informacji,
4) Zasady i procedury opisane w Polityce bezpieczeństwa informacji,
5) Zaobserwowane nieprawidłowości i wyniki kontroli.

Proces uświadamiania i kształcenia pracowników obejmuje również regularne przeprowadzanie szkoleń ze szczególnym uwzględnieniem zagadnień wskazanych powyżej.

Informacja o uczestnictwie w szkoleniu pracownika powinna znajdować się w aktach osobowych pracownika (zaświadczenie lub certyfikat).

Z przeprowadzonego szkolenia powinna zostać sporządzona lista obecności.

16. Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami

Monitorowanie dostępu do informacji realizowane jest poprzez:

1) logi aplikacji dziedzinowych,
2) logi systemów operacyjnych,
3) logi urządzeń zabezpieczających dostęp na styku sieci lokalnej i Internetu (UTM).

Powyższe informacje zawierają:

1) identyfikator i/lub adres IP komputera,
2) dokładną datę,
3) zakres dostępu (przydzielony/odrzucony),
4) opis wykonanej lub zablokowanej akcji.

a) Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji:

1) wdrożony System Data Leak Prevention (DLP),
2) ochronę antywirusową,
3) ochronę antyspamową;

b) Wprowadzenie blokady bezpośredniego dostępu stacji roboczych do sieci Internet:

1) umożliwia zablokowanie bezpośredniego połączenia złośliwego oprogramowania z sieci Internet,
2) utrudnia ominięcie systemów zabezpieczeń,
3) umożliwia kontrolę dostępu i rozliczalność działań użytkowników;

c) System informatyczny posiada wdrożony centralnie zarządzający system antywirusowy i antyspamowy, dzięki któremu:

1) ułatwione jest zarządzanie bezpieczeństwem stacji roboczych i poczty,

2) możliwe jest śledzenie bezpieczeństwa antywirusowego stacji roboczych.

a) Zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

Pracownicy na stacjach roboczych pracują z uprawnieniami ograniczonymi co blokuje bezpośredni dostęp do systemów operacyjnych.

Bazy danych znajdują się na serwerze (serwerach) co umożliwia bezpośredni (nieautoryzowany) do nich dostęp.

17. Umowy serwisowe

Zasady wskazane poniżej stosuje się do umów zawieranych podmiotami trzecimi o powierzenia o powierzenie danych do przetwarzania, jak również innych umów faktycznie udostępniających dane jednostki.

Umowy powinny zawierać:

a) klauzulę o zachowaniu poufności danych przekazanych przez Administratora Danych; klauzula powinna dotyczyć tak podmiotu, któremu dane powierzono, jak również osób upoważnionych do przetwarzania danych;
b) klauzulę wskazująca, tajemnica zachowania danych w poufności powinna zostać zachowana zarówno w trakcie trwania umowy, jak również po jej ustaniu;
c) zobowiązanie podmiotu, któremu powierzono przetwarzanie danych osobowych, do trwałego i protokolarnego usunięcia powierzonych danych w określonym terminie po zakończeniu przetwarzania danych;
d) klauzulę uprawniającą powierzającego do dokonywania kontroli prawidłowości przetwarzania danych (poprzez wgląd do dokumentacji oraz procedur);
e) kary umowne dla podmiotu, któremu powierzono dane, za każdorazowe naruszenie postanowień umowy w zakresie przetwarzania danych, jak również ponoszenia odpowiedzialności za szkodę wyrządzoną osobom trzecim z tego tytułu;
f) klauzulę dotyczącą wypowiedzenia umowy z zachowaniem terminów wypowiedzenia, albo bez zachowania terminów wypowiedzenia, w sytuacji w której podmiot, któremu powierzono

przetwarzanie danych osobowych narusza postanowienia ustawy, przepisów wykonawczych, albo umowy w tym zakresie;

g) klauzulę, że podmiot któremu dane zostały powierzone do przetwarzania (jak również podmioty mu podległe) zobowiązuje się do zachowania należytej staranności przy przetwarzaniu danych.

18. Zarządzanie incydentami naruszenia bezpieczeństwa informacji

Reagowanie na incydenty

Wszelkie zdarzenia związane z naruszeniem bezpieczeństwa informacji lub ujawnieniem podatności należy zgłaszać do: Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego, a w przypadku niemożliwości kontaktu z nimi do bezpośredniego przełożonego.

Każdy z pracowników w sytuacji gdy zauważy:

1. nieskuteczne zabezpieczenie;
2. naruszenie oczekiwanej integralności, poufności lub dostępności informacji;
3. błędy ludzkie wpływające na bezpieczeństwo informacji, zarówno swoje jak i współpracowników;
4. zachowania niezgodne z polityką lub zaleceniami;
5. naruszenia ustaleń związanych z bezpieczeństwem fizycznym;
6. nienadzorowane zmiany systemu;
7. niepoprawne działania systemu lub sprzętu;
8. naruszenia dostępu;
9. awarie lub inne nienormalne zachowania systemu mogące wskazywać na atak lub rzeczywiste naruszenie bezpieczeństwa .

Zobowiązany jest do możliwie najszybszego zgłaszania tychże zdarzeń Administratorowi Danych Osobowy, Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemu Informatycznego.

Postępowanie z incydentami

Administrator Bezpieczeństwa Informacji/Administrator Systemu Informatycznego dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie jako:

1) zdarzenie nie mające cech naruszenia bezpieczeństwa informacji, np. zaplanowana przerwa technologiczna,
2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej,
3) awaria techniczna czasowo blokująca dostępność informacji,
4) incydent niskiej, średniej lub wysokiej kategorii związany z naruszeniem bezpieczeństwa informacji, a szczególnie jej integralności, poufności i dostępności.

Analiza incydentu uwzględnia następujące kryteria:

1) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
2) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
3) liczba referatów/komórek organizacyjnych dotkniętych incydentem,
4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji,
5) możliwości rozszerzania się incydentu i sposoby jego ograniczania,
6) szacowany poziom szkód finansowych,
7) rodzaj ujawnionej informacji (jeśli ma zastosowanie - np. dane osobowe),
8) szacunkowy czas, po którym skutki incydentu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
9) skutki organizacyjne i prawne (wstępny szacunek).

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczegółowych.

1. Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe.
2. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których są dane osobowe, obowiązani są do przerwania pracy i w miarę możliwości przed opuszczeniem tych pomieszczeń do:
   a) zamknięcia systemu informatycznego,
   b) zabezpieczenia danych osobowych gromadzonych w kartotekach.
3. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Bezpieczeństwa Informacji oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczyć dane osobowe przed nieuprawnionym do nich dostępem.
4. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

21. Wykaz załączników

Załącznik nr 1 Wykaz budynków i pomieszczeń,

Załącznik nr 2 Wykaz i struktura zbiorów danych,

Załącznik nr 3 Sposób przepływu danych,

Załącznik nr 4 Oświadczenie o znajomości PBI i poufności informacji,

Załącznik nr 5 Upoważnienie,

Załącznik nr 6 Ewidencja osób upoważnionych do przetwarzania danych osobowych,

Załącznik nr 7 Wniosek o nadanie upoważnienia/uprawnienia do przetwarzania danych osobowych,

Załącznik nr 8 Dziennik zdarzeń i incydentów.

BURMISTRZ
TADEUSZ POGODA

Dokumentowanie i wyciąganie wniosków

Administrator Bezpieczeństwa Informacji/Administrator Systemu Informatycznego sporządza raport z zaistniałej sytuacji uwzględniające informacje wskazane powyżej oraz identyfikuje dane zdarzenie w rejestrze incydentów - **załącznik nr 8.**

Administrator Bezpieczeństwa Informacji/Administrator Systemu Informatycznego każdorazowo po wpisaniu nowego incydentu do rejestru analizuje poprzednie incydenty celem wykrycia ewentualnych powiązań pomiędzy nimi i podjęcia dodatkowych działań mających na celu minimalizację ryzyka jego ponownego wystąpienia.

Dodatkowo, incydenty mogą być wykorzystywane podczas szkoleń pracowniczych jako przykłady tego co może się wydarzyć, jak unikać ich w przyszłości i jak reagować jak się wydarzą. Podczas wykorzystywania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowania poufności.

19. Audyt wewnętrzny w zakresie bezpieczeństwa informacji

Podmioty realizujące zadania publiczne zobowiązane są do zapewniania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, bowiem utrzymywanie wysokiego poziomu bezpieczeństwa informacji, w tym systemu informatycznego wymaga stałego monitorowania i okresowego badania stanu zabezpieczenia wszystkich elementó tego systemu.

Administrator Systemu Informatycznego pod nadzorem Administratora Danych Osobowych, powinien nadzorować i wdrażać rekomendacje poaudytowe, zgodnie z ustalonym planem i priorytetami. Za nadzorowanie, wykonanie powyższego audytu odpowiada Administrator Bezpieczeństwa Informacji.

20. Postępowanie w wypadku klęski żywiołowej

Klęska żywiołowa jest katastrofą, spowodowaną działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

Załącznik nr 1 do Polityki bezpieczeństwa informacji	*Tytuł* **Wykaz budynków i pomieszczeń**

Budynek Urzędu Miejskiego w Świeciu znajduje się przy ulicy Wojska Polskiego 124. Obszar przetwarzania danych obejmuje zarówno miejsca, w których wykonuje się operacje na danych osobowych (np. wpisuje, modyfikuje, kopiuje), jak również miejsca, w których przechowuje się wszelkie nośniki (szafy z dokumentacją papierową szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco). Obszar przetwarzania danych nie obejmuje pomieszczeń i części pomieszczeń ww. budynku dostępnych dla osób trzecich takich jak: ciągi komunikacyjne - korytarze, hole, toalety, magazyny, pomieszczenia gospodarcze, pomieszczenia obsługi, poczekalnie itp.

Na obszar przetwarzania danych osobowych składają się następujące pokoje biurowe: 02, 2, 3, 7, 8, 9, 11, 12, 13, 14, 15, 17, 18, 24, 26, 27, 30. Natomiast Urząd Stanu Cywilnego znajduje się w Ratuszu Miejskim przy ulicy Duży Rynek 1.

Załącznik nr 2 do Polityki bezpieczeństwa informacji	*Tytuł* **Wykaz i struktura zbiorów danych**

1.

Nazwa zbioru:	**Dziennik korespondencji przychodzącej i wychodzącej**
Status zbioru:	Zbiór zwolniony z rejestracji na podstawie art. 43 ust.1 pkt 12.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	Imię, nazwisko, nazwa, adres korespondencyjny.

2.

Nazwa zbioru:	**Dziennik korespondencji Urzędu Stanu Cywilnego**
Status zbioru:	Zbiór zwolniony z rejestracji na podstawie art. 43 ust.1 pkt 12.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	Imię, nazwisko, nazwa, adres korespondencyjny.

3.

Nazwa zbioru:	**Rejestr wniosków o udzielenie informacji publicznej**
Status zbioru:	Zbiór zwolniony z rejestracji na podstawie art. 43 ust.1 pkt 12.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	Imię, nazwisko, nazwa, adres korespondencyjny, adres e-mail.

4.

Nazwa zbioru:	**Rejestr skarg, wniosków i petycji**
Status zbioru:	Zbiór zwolniony z rejestracji na podstawie art. 43 ust.1 pkt 12.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	Imię, nazwisko, treść skargi, wniosku, adres

5.

Nazwa zbioru:	**Kadry i Płace**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 4.
Forma przetwarzania danych:	Papierowa oraz za pomocą programu: KADRY i PŁACE U.I Infosystem, PŁATNIK „Prokom".
Struktura zbioru danych:	imię i nazwisko, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, korespondencyjny, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, dokumentacja kandydata do pracy, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, nr konta bankowego.

6.

Nazwa zbioru:	**Zakładowy Fundusz Świadczeń Socjalnych**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 4.
Forma przetwarzania danych:	Elektroniczna: pakiet MS Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, data i miejsce urodzenia, numer ewidencyjny PESEL, adres zamieszkania, numer konta bankowego, miejsce pracy, zawód, wykształcenie.

7.

Nazwa zbioru:	**Stażyści**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 4.
Forma przetwarzania danych:	Papierowa.
Struktura zbioru danych:	imię i nazwisko, data urodzenia, adres zamieszkania, adres korespondencyjny, numer ewidencyjny PESEL, miejsce odbywania stażu oraz zajmowane stanowisko, okres odbywania stażu.

8.

Nazwa zbioru:	**Rada Gminy**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust.1a.
Forma przetwarzania danych:	Papierowa oraz elektroniczna (publikacja na Biuletynie Informacji Publicznej).
Struktura zbioru danych:	imię, nazwisko, nazwisko rodowe, miejsce zatrudnienia, stanowisko lub funkcja, stan majątkowy, informacje o wynagrodzeniu, informacje o zajmowanym stanowisku kierowniczym w podmiotach prawa gospodarczego, adres zamieszkania; telefon kontaktowy.

9.

Nazwa zbioru:	**Gospodarka odpadami komunalnymi**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu informatycznego do obsługi gospodarki komunalnej oraz papierowa.
Struktura zbioru danych:	właściciel nieruchomości, imię, nazwisko, PESEL, data urodzenia, imię ojca, imię matki, numer telefonu

10.

Nazwa zbioru:	**Ochrona środowiska**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, nr ew. działki i położenie, obręb działki, tytuł władania nieruchomością, powierzchnia płyt azbestowych.

11.

Nazwa zbioru:	**Drogi/Inwestycje**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, nr ew. działki i położenie, nazwa firmy, adres zamieszkania adresata decyzji i innych stron postępowania, numer decyzji, data wydania decyzji, organ wydający decyzję, oznaczenie stron postępowania.

12.

Nazwa zbioru:	**Zamówienia publiczne**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres, Numer Identyfikacji Podatkowej, Nr REGON, numer konta bankowego, podwykonawcy, telefon kontaktowy.

13.

Nazwa zbioru:	**Obrona cywilna**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zameldowania, adres zamieszkania, data i miejsce urodzenia, miejsce pracy, numer telefonu, imiona rodziców, PESEL,

14.

Nazwa zbioru:	**Kwalifikacja wojskowa**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, PESEL, data i miejsce urodzenia, stan cywilny, adres i data zameldowania na pobyt stały, adres i data zameldowania na pobyt czasowy, numer i seria dowodu osobistego

15.

Nazwa zbioru:	**Kontrahenci indywidualni/Księgowość budżetowa**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 8.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office, systemu finansów-księgowego oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, nazwa, adres, siedziba, Numer Identyfikacji Podatkowej, Nr REGON, PESEL, nr konta bankowego, adres

16.

Nazwa zbioru:	**Ewidencja działalności gospodarczej**
Status zbioru:	Procesor
Forma przetwarzania danych:	Papierowa oraz elektroniczna za pomocą systemu CEiDG.
Struktura zbioru danych:	Płeć, rodzaj dokumentu tożsamości, serię i numer dokumentu tożsamości, PESEL, NIP, REGON, nazwisko, nazwisko rodowe, imię pierwsze, imię drugie, imię ojca, imię matki, miejsce urodzenia, data urodzenia posiadane obywatelstwo, pouczenie/oświadczenie, określenie czy jest się cudzoziemcem oraz dane dokumentu potwierdzającego status cudzoziemca, adres miejsca zamieszkania wnioskodawcy: województwo, powiat, gmina, miejscowość, ulica, nr nieruchomości/domu, nr lokalu, kod pocztowy, poczta, określenie firmy przedsiębiorcy, którego wniosek dotyczy, przewidywana liczba pracujących/zatrudnionych, rodzaj działalności gospodarczej nazwa skrócona, data rozpoczęcia działalności, dane do kontaktu: nr telefonu, faksu, adres poczty elektronicznej, strona www, główne miejsce wykonywania działalności gospodarczej jeżeli jest inne niż adres wnioskodawcy, dodatkowe miejsce wykonywania działalności: numer REGON, nazwa jednostki lokalnej, adres dodatkowego miejsca wykonywania działalności gospodarczej (podanie danych adresowych jak wyżej), data powstania obowiązku opłacania składek do ZUS, dane dla potrzeb KRUS, informacja o zawieszeniu/wznowieniu/zaprzestaniu wykonywania działalności gospodarczej, informacja dotycząca naczelników urzędów skarbowych, oświadczenie o formie opłacania podatku dochodowego od osób fizycznych, forma wpłaty zaliczki, rodzaj prowadzonej dokumentacji rachunkowej, dane podmiotu prowadzącego dokumentację rachunkowa wnioskodawcy (firma, NIP), adres miejsca przechowywania dokumentacji rachunkowej wnioskodawcy, wskazanie czy prowadzę: zakład pracy chronionej, zagraniczne przedsiębiorstwo drobnej wytwórczości, działalność w formie spółki/spółek cywilnych, jestem wspólnikiem spółki, informacje o małżeńskiej wspólności majątkowej, dane identyfikacyjne rachunków bankowych wnioskodawcy: kraj siedziby banku, pełna nazwa banku, posiadacz rachunku, nr rachunku, osobisty rachunek bankowy (dane jak poprzednio wskazane), pełnomocnictwo do prowadzenia spraw, dane pełnomocnika: wskazanie czy pełnomocnik jest osobą prawną, nazwa firmy pełnomocnika, imię i nazwisko, PESEL/KRS, data urodzenia, NIP, obywatelstwo, adres pełnomocnika (dane jak poprzednio wskazywane), zakres pełnomocnictwa

17.

Nazwa zbioru:	**Zezwolenia na sprzedaż napojów alkoholowych**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego MS Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, nazwa, adres zamieszkania (siedziba firmy), Numer Identyfikacji Podatkowej (NIP), numer telefonu, seria i numer dowodu osobistego, miejsce pracy, rodzaj zezwolenia, przedmiot działalności gospodarczej, numer w rejestrze przedsiębiorców, adres punktu sprzedaży/adres punktu składowania napojów alkoholowych, dane pełnomocników (imię, nazwisko, adres zamieszkania), adres zamieszkania (lub siedziby).

18.

Nazwa zbioru:	**Podatki i opłaty lokalne**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pośrednictwem systemu podatkowego Infosystem, KASA Infosystem, SYSTEmEG Egzekucje oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, data urodzenia, adres, numer i seria dowodu osobistego, imiona rodziców, informacja o wysokości i rodzaju podatku, adres nieruchomości, numer nieruchomości, numer księgi wieczystej, NIP, nr konta bankowego, PESEL, kwota zadłużenia lub dane dot. należności pieniężnych, dane dot. zaistnienia zdarzenia z którym ustawa podatkowa wiąże powstanie zobowiązania podatkowego, marka pojazdu, typ, model, liczba osi, rok produkcji pojazdu, dane dotyczące własności/współwłasności pojazdu, tytuł prawny do nieruchomości, tytuły wykonawcze, wysokość zaległości, wysokość odsetek, ilość zakupionego paliwa, kwota zwrotu podatku, limit zwrotu podatku

19.

Nazwa zbioru:	**Rolnictwo**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa
Struktura zbioru danych:	imię, nazwisko, adres zamieszkania, numer polisy ubezpieczeniowej, dane dot. nieruchomości.

20.

Nazwa zbioru:	**Zagospodarowanie przestrzenne**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego MS Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, nr ew. działki i położenie, imiona rodziców.

21.

Nazwa zbioru:	**Gospodarowanie zasobem mieszkaniowym**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego MS Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, data urodzenia, adres zamieszkania, adres zamieszkania, seria i numer dowodu osobistego, PESEL, numer telefonu, wysokość i źródło dochodu, warunki zamieszkiwania kwalifikujące do ich poprawy, tytuł prawny do lokalu, ilość członków rodziny, inne informacje zawarte we wniosku osób ubiegających się o lokal socjalny lub zamianę lokalu, powierzchnia lokalu socjalnego lub użytkowego.

22.

Nazwa zbioru:	**Gospodarka nieruchomościam**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, imiona rodziców, data i miejsce urodzenia, PESEL, numer i seria dowodu osobistego, adres zamieszkania, nr ew. działki i położenie, inne informacje dotyczące nieruchomości – powierzchnia, wartość, przeznaczenie, wysokość naliczonych opłat z tytułu dzierżawy, wieczystego użytkowania, terminy płatności), okres dzierżawy, numer księgi wieczystej, numer dokumentu będącego podstawą prawa własności.

23.

Nazwa zbioru:	**Rejestr dowodów osobistych**
Status zbioru:	Procesor
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło oraz papierowa.
Struktura zbioru danych:	numer PESEL, nazwisko i imię (imiona), nazwisko rodowe, imię ojca, imię i nazwisko rodowe matki, data i miejsce urodzenia, płeć, wzrost, kolor oczu, adres miejsca zamieszkania na pobyt stały/pobyt czasowy trwający ponad 3 m-c, seria i numer poprzedniego dowodu, wystawca dowodu, wizerunek twarzy, podpis wnioskodawcy.

24.

Nazwa zbioru:	**Rejestr mieszkańców**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło, systemu ARAM oraz papierowa.

Struktura zbioru danych:	nazwisko i imię (imiona), nazwisko rodowe, imiona i nazwiska rodowe rodziców, data urodzenia, miejsce urodzenia, kraj urodzenia, stan cywilny, numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, płeć, numer PESEL, obywatelstwo albo status bezpaństwowca, imię i nazwisko rodowe oraz numer PESEL małżonka, jeżeli został mu nadany, data zawarcia związku małżeńskiego, numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, data rozwiązania związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt oznaczenie sądu, który ustalił nieistnienie małżeństwa, sygnatura akt oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, numer jego aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, adres i data zameldowania na pobyt stały; kraj miejsca zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z miejsca pobytu stałego, adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu, data wymeldowania z miejsca pobytu czasowego, data wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy i wskazanie kraju wyjazdu, data powrotu z wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy, seria, numer i data ważności ostatniego wydanego dowodu osobistego obywatela polskiego oraz oznaczenie organu wydającego dokument, seria, numer i data ważności ostatniego wydanego paszportu obywatela polskiego, data zgonu albo data znalezienia zwłok, numer aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony.

25.

Nazwa zbioru:	**Rejestr zamieszkałych cudzoziemców**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło, systemu ARAM oraz papierowa.
Struktura zbioru danych:	nazwisko i imię (imiona), data urodzenia, kraj urodzenia, płeć, numer PESEL, obywatelstwo albo status bezpaństwowca, adres i data zameldowania na pobyt stały, kraj miejsca zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z miejsca pobytu stałego, seria, numer i data ważności dokumentu podróży cudzoziemca, a w przypadku cudzoziemców, o których mowa w art. 7 ust. 1 pkt 3 lit. a i b,

	ważnego dokumentu podróży lub innego ważnego dokumentu potwierdzającego tożsamość i obywatelstwo; Pozostałe dane o ile są dostępne, mianowicie: imiona i nazwiska rodowe rodziców, miejsce urodzenia, stan cywilny, numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, imię i nazwisko rodowe oraz numer PESEL małżonka, jeżeli został mu nadany, data zawarcia związku małżeńskiego, numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, data rozwiązania, związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt i oznaczenie sądu, który ustalił nieistnienie małżeństwa, sygnatura akt i oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, numer jego aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu, data wymeldowania z miejsca pobytu czasowego, data wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6miesięcy i wskazanie kraju wyjazdu, data powrotu z wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy, data upływu deklarowanego przez cudzoziemca terminu pobytu, data zgonu albo data znalezienia zwłok, numer aktu zgonu i oznaczenie, urzędu stanu cywilnego, w którym ten akt został sporządzony.

26.

Nazwa zbioru:	**Akta Stanu Cywilnego**
Status zbioru:	Zbiór podlega zgłoszeniu do rejestracji GIODO z uwagi na art. 27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło, systemu ARAM oraz papierowa.
Struktura zbioru danych:	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, nazwisko: panieńskie, z poprzedniego małżeństwa, rodowe, miejsce i godzina urodzenia, data i numer aktu: urodzenia, małżeństwa, zgonu, nazwisko i imię: ojca, matki, współmałżonka, płeć, stan cywilny, data i miejsce zawarcia małżeństwa, nazwisko i imię, adres osoby zgłaszającej zgon, numer aktu zgonu żony, męża, imię i nazwisko rodowe małżonka, nazwisko rodowe matki i ojca kobiety, mężczyzny, data unieważnienia aktu małżeństwa, urodzenia, zgonu, imię nadane z urzędu, data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo,

	przysposabiającego dziecko, imię i nazwisko przysposabiającej dziecko, zmiana nazwiska dziecka, rejestracja w polskich księgach stanu.

27.

Nazwa zbioru:	**Gminna Komisja Rozwiązywania Problemów Alkoholowych**
Status zbioru:	Zbiór podlega zgłoszeniu do rejestracji GIODO z uwagi na art. 27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego MS Office oraz papierowa
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, status rodzinny, źródło i wysokość dochodów, wykształcenie, PESEL, data urodzenia, **dane wrażliwe: stan zdrowia, nałogi.**

28.

Nazwa zbioru:	**Nieodpłatna kontrolowana praca fizyczna na cele społeczne przydzielona przez Sąd**
Status zbioru:	Zbiór podlega zgłoszeniu do rejestracji GIODO z uwagi na art. 27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, okres wykonywania kary, orzeczenie o skazaniu.

29.

Nazwa zbioru:	**Rejestr wyborców**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust. 1 pkt 6.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu ministerialnego Źródło, systemu WYB+A oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, imię ojca, data urodzenia, PESEL, adres zamieszkania.

30.

Nazwa zbioru:	**Karta Dużej Rodziny**
Status zbioru:	Zbiór podlega zgłoszeniu do rejestracji GIODO z uwagi na art. 27 ust. 1.
Forma przetwarzania danych:	W postaci papierowej oraz dane z wniosków są wprowadzane do systemu SI KRD.
Struktura zbioru danych:	imię, nazwisko, data urodzenia, adres zamieszkania, adres korespondencyjny, PESEL, numer dokumentu, numer telefonu, stan zdrowia, orzeczenie o umiarkowanym lub znacznym stopniu niepełnosprawności oraz termin, ważności orzeczenia potwierdzającego te okoliczności, jeżeli termin taki wskazano, informacja o umieszczeniu w rodzinie zastępczej oraz termin do którego dziecko zostało umieszczone w rodzinnej pieczy zastępczej, jeżeli termin taki wskazano, informacja o pozostawaniu w dotychczasowej rodzinie zastępczej lub rodzinnym domu dziecka, zaświadczenie ze szkoły lub szkoły wyższej o planowanym terminie ukończenia nauki w danej placówce.

31.

Nazwa zbioru:	**Świadczenia rodzinne**
Status zbioru:	Zbiór podlega rejestracji do GIODO z uwagi na art.27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu informatycznego SYGNITY oraz papierowa.
Struktura zbioru danych:	Imię i nazwisko, PESEL, data urodzenia, stan cywilny, adres zamieszkania/korespondencyjny, numer telefonu, nr rachunku bankowego, kwota świadczenia na rzecz innych osób, NIP, miejsce pracy, zawód wykształcenie, seria i numer dowodu osobistego, stan zdrowia, nałogi, orzeczenia wydane w postępowaniu sądowym i administracyjnym, stan cywilny, dochody, zaświadczenia lekarskie, nazwa banku, ilość dzieci, wiek dzieci, miejsce nauki dzieci, dochody dzieci, akt zgonu rodzica lub dziecka, zaświadczenia lekarskie, z urzędu skarbowego, od pracodawcy, orzeczenie o niepełnosprawności, kwoty alimentów świadczonych na rzec innych osób

32.

Nazwa zbioru:	**Dodatki mieszkaniowe**
Status zbioru:	Zbiór podlega rejestracji do GIODO z uwagi na art.27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu informatycznego SYGNITY oraz papierowa.
Struktura zbioru danych:	Imię i nazwisko, imiona rodziców, data urodzenia, PESEL, miejsce pracy, seria i numer dowodu osobistego, numer telefonu, miejsce pracy, zawód wykształcenie, tytuł prawny do zajmowanego lokalu, informacje o członkach rodziny, źródła dochodu, miesięczne wydatki, stan zdrowia,

33.

Nazwa zbioru:	**Rodzina 500+**
Status zbioru:	Zbiór podlega rejestracji do GIODO z uwagi na art.27 ust. 1.
Forma przetwarzania danych:	Elektroniczna- SW Sygnity, Papierowa
Struktura zbioru danych:	Imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, PESEL, NIP, imiona rodziców, miejsce pracy, zawód, seria i numer dowodu osobistego, numer telefonu, stan zdrowia, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym zaświadczenia z: Urzędu Gminy/Miasta, ZUS, KRUS, US, Urzędu Pracy, zakładów pracy, komornika sądowego, akty urodzenia, małżeństwa, zgonu, stan cywilny, stopień pokrewieństwa, obywatelstwo, płeć , dane konta bankowego, dochody rodziny, umowy dzierżawy, dowody wpłat alimentów, świadectwa pracy, wyrok sądu o zasądzonych alimentach, zeznania o wysokości osiągniętego dochodu, informacje o dochodach oraz o pobranych zaliczkach na podatek dochodowy, numer identyfikujący osobę mającą status cudzoziemca

34.

Nazwa zbioru:	**Rejestr mandatów i wykroczeń**
Status zbioru:	Zbiór podlega rejestracji do GIODO z uwagi na art.27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą programu Infosystem, CEPIK – mandaty oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, numer ewidencyjny PESEL, numer i seria dowodu osobistego, numer telefonu, mandaty karne, orzeczenia wydane w postępowaniu sądowym lub administracyjnym

35.

Nazwa zbioru:	**Budżet Obywatelski**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, numer ewidencyjny PESEL

36.

Nazwa zbioru:	**Archiwum**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 12.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	Wszystkie dane występujące w zbiorach opisanych w niniejszym wykazie.

Załącznik nr 3 do Polityki bezpieczeństwa informacji	*Tytuł* **Sposób przepływu danych pomiędzy systemami informatycznymi przetwarzającymi dane osobowe**

Systemy informatyczne (programy) przetwarzające dane osobowe zostały wymienione w załączniku nr 2 do Polityki bezpieczeństwa informacji.

Przepływ danych zachodzi pomiędzy systemem (programem) Płace a Płatnikiem, jest to przepływ jednokierunkowy.

Załącznik nr 4 do Polityki bezpieczeństwa informacji	*Tytuł* **Oświadczenie o znajomości Polityki bezpieczeństwa informacji i zachowaniu w poufności informacji**

OŚWIADCZENIE

Oświadczam, iż *zostałam/zostałem *zaznajomiona/zaznajomiony z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922), wydanych na jej podstawie aktów wykonawczych oraz wdrożonej **Polityki bezpieczeństwa informacji** oraz zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miała/miał* dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych, zarówno w trakcie obowiązującego stosunku pracy, jak i bezterminowo po ustaniu zatrudnienia.

Ponadto oświadczam, iż zostałam/zostałem zaznajomiona/zaznajomiony z faktem, iż systemy informatyczne, do których mam dostęp na komputerach służbowych i na których wykonuję obowiązki pracownicze, są monitorowane, w zakresie ilościowego i jakościowego wykorzystania tych systemów.

Oświadczam, że monitoring obejmuje również sposób wykorzystania służbowej poczty elektronicznej. Zobowiązuję się do wykorzystywania jej jedynie w celu realizacji zadań pracowniczych, wynikających ze stosunku pracy.

(podpis osoby składającej oświadczenie)

* - niepotrzebne skreślić

……..,……r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn.zm.) upoważniam:

Pana/ Panią _____

Zatrudnionego/zatrudnioną w _____ do przetwarzania danych osobowych w celach związanych z wykonywaniem obowiązków służbowych, na stanowisku: _____ oraz zawartych w następujących zbiorach danych:

Nazwa zbioru danych	O*	M*
1.		
2.		
3.		
4.		

*O - odczyt danych,

*M - modyfikacja danych (wprowadzanie, zmienianie, usuwanie).

Upoważnienie obowiązuje na czas zajmowania ww. stanowiska. Ponadto w każdym czasie może zostać zmienione lub odwołane.

_____

(pieczęć administratora danych)

Niniejszym uprzednio wydane upoważnienie traci moc.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	**Imię i nazwisko**	**Stanowisko/Funkcja**	**Data nadania**	**Data ustania**	**Zakres upoważnienia**	**Identyfikator**

.....

(Podpis osoby upoważnionej do prowadzenia ewidencji)

Załącznik nr 7 do Polityki bezpieczeństwa informacji	*Tytuł* **Wniosek o nadanie upoważnienia/uprawnienia do przetwarzania danych osobowych**

Wniosek o nadanie upoważnienia/uprawnienia do przetwarzania danych osobowych

Nr upoważnienia:

Wnioskuje o przyznanie / odebranie upoważnienia do przetwarzania danych osobowych dla:

1. Imię:.....
2. Nazwisko: .....
3. Stanowisko służbowe:.....
4. Nazwa komórki organizacyjnej: .....
5. Okres obowiązywania upoważnienia:.....

Lp.	Zbiór danych osobowych	Forma[1]	Systemy Informatyczne[2]	Uprawnienia
1.	Dziennik korespondencji przychodzącej i wychodzącej			
2.	Rejestr wniosków o udzielenie informacji publicznej			
3.	Rejestr skarg i wniosków			
4.	Kadry i Płace			
5.	Wykaz Radnych i Sołtysów			
6.	Gospodarka odpadami komunalnymi			
7.	Ochrona środowiska			
8.	Decyzje drogowe			
9.	Zamówienia publiczne			
10.	Obrona cywilna			
11.	Rejestr osób podlegających rejestracji i kwalifikacji wojskowej			
12.	Kontrahenci			
13.	Rejestr wniosków o wpis do CEiDG			
14.	Zezwolenia na sprzedaż napojów alkoholowych			
15.	Podatki i opłaty lokalne			
16.	Rolnictwo			
17.	Zagospodarowanie przestrzenne			
18.	Ewidencja najemców i właścicieli lokali – gospodarowanie zasobem mieszkaniowym			
19.	Gospodarka nieruchomościami			
20.	Rejestr dowodów osobistych			
21.	Rejestr mieszkańców			

22.	Rejestr zamieszkałych cudzoziemców			
23.	Akta Stanu Cywilnego			
24.	Woda i ścieki			
25.	Karta Dużej Rodziny			
26.	500 Plus			
27.	Monitoring wizyjny			
28.	Rejestr petycji			
29.	Archiwum zakładowe			

[1] Forma przetwarzania – (E) elektroniczna, tradycyjna, papierowa (T)
[2] Systemy informatyczne korzystające z danego zbioru danych
[3] W przypadku ubiegania się o nadanie uprawnienia wpisz „TAK", w przeciwnym razie wpisz „NIE".

Upoważniam/Nie upoważniam wskazaną osobę do dostępu do danych osobowych w wyżej opisanym zakresie.

.....

(data i czytelny podpis Administratora Danych Osobowych lub osoby upoważnionej)

Załącznik nr 8 do Polityki bezpieczeństwa informacji	*Tytuł* **Dziennik zdarzeń/incydentów**

Data wystąpienia incydentu	**Rodzaj incydentu**	**Osoba, która przyczyniła się do wystąpienia incydentu**	**Podjęte działania**	**Osoba podejmująca działanie**	**Stopień zagrożenia**