Załącznik Nr 1
do Zarządzenia Burmistrza Gminy i Miasta Witkowa
Nr 9 z dnia 21 stycznia 2016r.

POLITYKA BEZPIECZEŃSTWA

DANYCH OSOBOWYCH

URZĘDU GMINY I MIASTA W WITKOWIE

Rozdział I

POSTANOWIENIA OGÓLNE

§ 1. **Polityka bezpieczeństwa** została opracowana zgodnie z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2015 r. poz.2135) oraz 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. z 2004 r. Nr 100, poz. 1024).

§ 2. Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Witkowie.

§ 3. Ilekroć w Polityce jest mowa o:

1) **jednostce organizacyjnej** - rozumie się przez to Urząd **Gminy i Miasta w Witkowie**;
2) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **przetwarzaniu danych - rozumie** się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
5) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków

trwałych w celu przetwarzania danych osobowych na papierze (zewidencjonowany, usystematyzowany zbiór kartotek, wykazów, skoroszytów i innej dokumentacji gromadzonej w formie papierowej zawierającej dane osobowe);

7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to **Burmistrza** - kierownika jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;
10) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)** - rozumie się przez to osobę wyznaczoną przez Burmistrza, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi ADO;
11) **„Informatyka”** zwanym też **Administratorem Systemu Informatycznego (ASI)** - rozumie się przez to osobę zatrudnioną przez Burmistrza do realizacji zadań związanych z zarządzaniem systemem informatycznym odpowiedzialną m.in.: za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację;
12) **komórce organizacyjnej** - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym;
13) **kierownik komórki organizacyjnej –** rozumie się również samodzielne stanowisko pracy;
14) **użytkowniku –** rozumie się przez to osobę wyznaczoną przez Burmistrza lub osobę przez niego upoważnioną do przetwarzania danych osobowych w systemie informatycznym lub kartotekach;

15) **zgodzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
16) **pomieszczeniach** - rozumie się prze to 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 kartotekach.

Rozdział II
CELE

§ 4. Dane osobowe w Urzędzie Gminy i Miasta w Witkowie są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Urzędu Gminy i Miasta na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 5. Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:
1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

§ 6. Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.

§ 7. Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Urzędu Gminy i Miasta w Witkowie, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Witkowie (np.: osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów).

§ 8.1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji.

§ 9.1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie;
2) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach 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.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 10.1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie;
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach 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, jeżeli nawet przetwarzanie jest niezbędne

do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą;

6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 11. Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy komórek organizacyjnych.

§ 12.1. Z zasadami w Polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik **Nr 1** do Polityki.

2. Oświadczenie przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ADO.

§ 13.1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Urzędu Gminy i Miasta w Witkowie oraz osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik **Nr 2** do niniejszej polityki. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla komórek organizacyjnych Urzędu Gminy i Miasta w Witkowie.

2. Upoważnienie określone w ust. 1 przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji ADO.

3. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi pracownik ds. kadrowych.

4. Wzór ewidencji określonej w ust. 2 stanowi załącznik **Nr 3** do Polityki bezpieczeństwa.

§ 14.1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w jednostce organizacyjnej dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi.

Rozdział III
ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§15.1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO).

2. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§16.1. Administrator Danych Osobowych może powołać Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 17.1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.

3. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

4. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 1 i 2 ustawy o ochronie danych osobowych, oraz przestrzegania zasad w niej określonych;

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (szkolenia).

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy o ochronie danych osobowych, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 ustawy o ochronie danych osobowych.

3) nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;
4) nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;
5) weryfikuje listę autoryzowanych użytkowników systemów informatycznych;
6) doradza użytkownikom w zakresie bezpieczeństwa;
7) dba, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa;
8) prowadzi kontrolę w zakresie bezpieczeństwa;
9) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych;
10) przygotowuje wnioski pokontrolne dla Administratora Danych Osobowych;
11) prowadzi rejestr zbiorów danych osobowych przetwarzanych przez administratora danych.

§ 18.1. Administrator Danych Osobowych wyznacza „Informatyka”- Administratora Systemu Informatycznego (ASI), który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.

3. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Systemu Informatycznego jest następujący:

1) zapewnia stałą sprawność urządzeń mających wpływ na bezpieczeństwo danych;
2) odpowiada za bezpieczeństwo systemu informatycznego;
3) zobowiązuje i bieżąco kontroluje stosowanie się użytkowników do obowiązujących procedur;
4) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego;
5) zapewnia aktualizację dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności;
6) prowadzi nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;
7) wykonuje kopie awaryjne/archiwalne /oraz nadzoruje ich przechowywanie;
8) wprowadza i nadzoruje mechanizmy autoryzacji.

§ 19. Kierownik komórki organizacyjnej odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników;
2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie;
3) zgłasza ADO planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie;
4) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom;

5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Urzędzie Gminy i Miasta w Witkowie.

§ 20. Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Danych Osobowych za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

Rozdział IV
WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§ 21. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik **Nr 4** do Polityki bezpieczeństwa.

§ 22. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Urzędzie wyróżnia się dwie kategorie danych:

1) **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych;
2) **dane osobowe szczególnie chronione** – zgodnie z art.27 ust.1 ustawy o ochronie danych osobowych (art. 27 ust. 1) wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie

zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 23. Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na gromadzone kategorie zbiorów danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1i 1a tejże ustawy.

Rozdział V

WYKAZ BUDYNKÓW TWORZĄCYCH OBSZAR PRZETWARZANIA DANYCH

§ 24. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych.

§.25. Obszarem przetwarzania danych są budynki, pomieszczenia lub ich części, w których przetwarzane są dane osobowe, znajdujące się w siedzibie Urzędu, ul. Gnieźnieńska 1, 62-230 Witkowo, gdzie zlokalizowane są komórki organizacyjne Urzędu, główne systemy informatyczne, archiwa, kartoteki, z wyłączeniem pomieszczeń socjalno i ogólnie dostępnych, tj. korytarzy, toalet, magazynków, pomieszczeń gospodarczych itp.

§ 26. Przetwarzanie danych jest zabronione, jeśli nie są zapewnione warunki ochrony danych osobowych określone w niniejszej Polityce.

Rozdział VI

OPIS STRUKTURY ZBIORÓW DANYCH OSOBOWYCH

§ 27. Szczegółowy opis struktury zbiorów danych osobowych określonych w załączniku nr 4 wraz ze wskazaniem poszczególnych pól informacyjnych i powiazań między nimi znajduje się w dokumentacji technicznej będącej w posiadaniu autorów oprogramowania.

§ 28. Programem wykorzystywanym do przetwarzania danych osobowych u Administratora Danych jest również pakiet biurowy Office.

§ 29. Dane osobowe przetwarzane są w aplikacjach:

a. edytor tekstu,
b. arkusz kalkulacyjny,
c. program pocztowy,

§ 30. Aplikacje pakietu Office oferują szeroki zakres możliwości rejestrowania:

a. daty wprowadzania danych,
b. identyfikatora użytkownika,
c. źródła danych,

uzależniony od konfiguracji, wersji, zainstalowanych składników, aktualizacji oraz poprawek.

§ 31. Aplikacją wykorzystywaną do przetwarzania danych w zbiorze „Kandydaci" jest również program pocztowy.

§ 32. Program pocztowy pozwala na różne możliwości przepływu danych pomiędzy aplikacjami, od bezpośredniego udostępniania danych bezpośrednio z modułu „Kontakty" poprzez dowolny eksport wybranych pól informatycznych do plików w standardowych formatach pozwalających na import danych do dowolnych aplikacji obsługujących te formaty.

§ 33. Zakres przetwarzania danych osobowych jest uzależniony od informacji jakie dobrowolnie udzieli kandydat. Informacje znajdują się w załącznikach do listu elektronicznego stanowiącego pliki: doc., rtf., pdf. Itp. oraz informacje przesyłane automatycznie z listem, które mogą być rejestrowane w module „Kontakty".

§ 34. Informacje zawarte w module „Kontakty" przechowywane są w pliku o domyślnej nazwie backup.pst zawierającym następujące pola informacyjne:

1. Nazwa:
   a) Tytuł
   b) Imię
   c) Drugie imię
   d) Nazwisko
   e) Sufiks
2. Firma
3. Dział
4. Stanowisko
5. Adres służbowy:
   a) Adres służbowy ulica
   b) Adres służbowy ulica2
   c) Adres służbowy ulica3
   d) Adres służbowy miejscowość
   e) Adres służbowy województwo
   f) Adres służbowy kod pocztowy
   g) Adres służbowy kraj
6. Adres domowy:
   a) Adres domowy ulica
   b) Adres domowy ulica2
   c) Adres domowy ulica3
   d) Adres domowy miejscowość
   e) Adres domowy województwo
   f) Adres domowy kod pocztowy
   g) Adres domowy kraj
7. Inny adres:
   a) Inny adres ulica
   b) Inny adres ulica2
   c) Inny adres ulica3
   d) Inny adres miejscowość
   e) Inny adres województwo
   f) Inny adres kod pocztowy
   g) Inny adres kraj
8. Telefon asystenta
9. Faks służbowy
10. Telefon służbowy
11. Telefon służbowy2
12. Wywołanie zwrotne
13. Telefon w samochodzie
14. Główny telefon do firmy
15. Faks domowy
16. Telefon domowy
17. Telefon domowy2
18. ISDN
19. Telefon komórkowy
20. Inny faks

21. Inny telefon
22. Pager
23. Telefon podstawowy
24. Radiotelefon
25. Telefon TTYTDD
26. Teleks
27. Adres e-mail:
    a) Adres poczty e-mail
    b) Typ poczty email
    c) Wyświetlana nazwa e-mail
28. Adres e-mail2:
    a) Adresemail2
    b) Rodzajemail2
    c) Wyświetlananazwaemail2
29. Adres e-mail3:
    d) Adresemail3
    e) Rodzajemail3
    f) Wyświetlananazwaemail3
30. Charakter
31. Domowa skrzynka pocztowa
32. Dzieci
33. Hobby
34. Imię i nazwisko asystenta
35. Informacje rozliczeniowe
36. Inicjały
37. Inna skrzynka pocztowa
38. Internetowe informacje wolny zajęty
39. Język
40. Kategorie
41. Konto
42. Lokalizacja
43. Lokalizacja biura
44. Menedżer
45. Notatki
46. Numer ewidencyjny w organizacji
47. Osoba polecająca
48. PESEL
49. Płeć
50. Priorytet
51. Prywatne
52. Przebieg
53. Rocznica
54. Serwer katalogowy
55. Słowa kluczowe
56. Służbowa skrzynka pocztowa
57. Strona sieci Web

58. Urodziny
59. Uzytkownik1
60. Uzytkownik2
61. Uzytkownik3
62. Użytkownik4
63. Współmałżonek
64. Zawód
65. Załączniki

Rozdział VII

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 35.1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki, winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.

Rozdział VIII

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 36.1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administrator Systemu Informatycznego zapewniający jego prawidłową eksploatację.

2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych.

3. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.

4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Rozdział IX
UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 37.1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

1) jakie dane osobowe zawiera zbiór;
2) w jaki sposób zebrano dane;
3) w jakim celu i zakresie dane są przetwarzane;
4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 38.1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące;
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;
7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą;
8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;
9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1 - 5, nie częściej niż raz na 6 miesięcy.

§ 39.1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego

lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować ADO.

§ 40.1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.

2. W przypadku udostępniania danych osobowych administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 41. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO z uwzględnieniem wymagań określonych w art.31 ust.1 ustawy o ochronie danych osobowych.

Rozdział X
ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 42. Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.

§ 43.1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

2. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział XI
BEZPIECZEŃSTWO FIZYCZNE

§ 44. Dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerach i w postaci tradycyjnej .

§ 45. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 46. Pomieszczenia, w których znajdują się systemy informacji winny być:
wyposażone w szafy, meble biurowe zamykane na klucz umożliwiające
przechowywanie dokumentów,
zamknięte, jeśli nikt w nich nie przebywa.

§ 47. Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą kierownika komórki organizacyjnej, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

Dział XII
BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 48. Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

§ 49. Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika komórki organizacyjnej.

§ 50. Zabrania się korzystania z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 51.1. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane w porozumieniu z ASI powinna dokonać zmiany hasła.

§ 52.1. Elektroniczne bazy danych osobowych są archiwizowane.

2. Kopie są wykonywane na nośnikach magnetycznych.

§ 53. Używanie oprogramowania prywatnego w sieci jest zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

Rozdział XIII
KONSERWACJE I NAPRAWY

§ 54. Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

§ 55.1. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.

2. Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest kierownik komórki organizacyjnej. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu Informatycznego.

§ 56. Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

1) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w pomieszczeniu biurowym znajdującym się w strefie o ograniczonym dostępie;
2) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

Dział XIV
PLANY AWARYJNE I ZAPOBIEGAWCZE

§ 57. Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

§ 58. W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na dwa tygodnie. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych, i przechowywane są przez Administratora Systemu Informatycznego. Użycie kopii zapasowych następuje na polecenie Administratora Systemu Informatycznego w przypadku odtwarzania systemu po awarii.

Rozdział XV
POLITYKA ANTYWIRUSOWA

§ 59. 1. Wszystkie serwery i komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

1) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;
2) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

2. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem sieci lokalnej.

Rozdział XVI

PRZEPISY KOŃCOWE

§ 60. Za naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

§ 61. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2015 r. poz.2135) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100, poz. 1024).

Załącznik Nr 1
do Polityki Bezpieczeństwa Danych Osobowych
Urzędu Gminy i Miasta w Witkowie

- W Z Ó R –

O Ś W I A D C Z E N I E

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Oświadczam, iż zostałam/zostałem zaznajomiona/zaznajomiony* z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2015 r. poz. 2135), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Polityką bezpieczeństwa danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Jednocześnie zobowiązuję się do ich przestrzegania.

....
(imię, nazwisko i podpis osoby przyjmującej oświadczenie) *(data i podpis składającego* oświadczenie)

……

(miejscowość, data)

*niepotrzebne skreślić

Załącznik Nr 2
do Polityki Bezpieczeństwa Danych Osobowych
Urzędu Gminy i Miasta w Witkowie

- W Z Ó R –

U P O W A Ż N I E N I E **Nr ……**

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2015 r. poz.2135), zgodnie z zakresem czynności i złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych.

U p o w a ż n i a m

Pana/Panią:

……

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/ tradycyjnym w ……
(nazwa komórki organizacyjnej)

w zbiorach :

Lp.	PEŁNA NAZWA ZBIORU

Powyższe upowaźnienie wydaje się na okres do ……..…..
(wpisać na jaki okres lub bezterminowo)

Upoważnienie obejmuje prawo wglądu bez prawa wprowadzania, modyfikowania i usuwania danych osobowych.*	Upoważnienie obejmuje prawo wglądu, wprowadzania modyfikowania i usuwania danych osobowych.*

* Zaznacz właściwe stawiając znak „x „ w odpowiedniej kolumnie .

Administrator Danych Osobowych

…… ……
/miejscowość/, data) *(Podpis)*

Załącznik Nr 3
do Polityki Bezpieczeństwa Danych Osobowych
Urzędu Gminy i Miasta w Witkowie

- W Z Ó R –

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

L.p.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login/ identyfikator	uwagi
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Zakres upoważnienia:
d- wgląd;
w- wprowadzanie:
m- modyfikacja:
u-usuwanie.

…..……..

(podpis osoby odpowiedzialnej za prowadzenie ewidencji)

Załącznik Nr 4
do Polityki Bezpieczeństwa Danych Osobowych
Urzędu Gminy i Miasta w Witkowie

- W Z Ó R –

WYKAZ ZBIORÓW DANYCH OSOBOWYCH I PROGRAMÓW W KTÓRYCH SĄ PRZETWARZANE

L.p.	Nazwa zbioru	Nazwa programu

Stan na dzień ……..r.

……
(podpis Administratora Danych)

Załącznik Nr 2
do Zarządzenia Burmistrza Gminy i Miasta Witkowa
Nr 9 z dnia 21 stycznia 2016r.

ISTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

URZĘDU GMINY I MIASTA W WITKOWIE

ROZDZIAŁ I

Postanowienia ogólne

§1.

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, a także zasady i tryb postepowania Administratora Danych oraz osób przez niego upoważnionych przy przetwarzaniu danych osobowych.
2. Instrukcja została opracowana zgodnie z wymogami określonymi w § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

§2

Instrukcja określa stosowne procedury i warunki zarządzania systemem informatycznym oraz kartotekami, zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

§3

1. Ilekroć w Instrukcji jest mowa o:
   1) **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
   2) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

3) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

4) **kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór, wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe;

5) **Administratorze Danych** – rozumie się prze to Urząd Gminy i Miasta w Witkowie;

6) **Burmistrzu** – rozumie się przez to Burmistrza Gminy i Miasta w Witkowie;

7) **Administratorze Bezpieczeństwa Informacji (ABI)** – rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenie danych przed ich udostepnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2015r.poz.2135) oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych;

8) **Administratorze Systemu Informatycznego (ASI)**-osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwacje – rozumie się przez to wyznaczonego przez Burmistrza informatyka odpowiedzialnego za powyższe zadania, zwanego dalej **„Informatykiem”;**

9) **komórce organizacyjnej** - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym;

10) **użytkowniku** – rozumie się przez to osobę wyznaczoną przez Burmistrza lub osobę przez niego upoważnioną do przetwarzania danych osobowych w systemie informatycznym oraz kartotekach;

11) **pracowniku ochrony** – rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych;

12) **pomieszczeniach** – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego lub gromadzone w kartotekach.

§4

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemu informatycznego.
2. W celu zwiększania efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
3. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) poufność danych – rozumianą, jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą, jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych – rozumianą, jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu – rozumianą, jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
4. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek oraz osoby na stanowiskach samodzielnych.

§5

1. W celu uwzględnienia ewentualnych zagrożeń oraz kategorii przetwarzanych danych wprowadzone zostały następujące poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:
   1) Podstawowy;
   2) Podwyższony;
   3) wysoki.
2. Poziom co najmniej podstawowy stosuje się gdy:
   1) w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy o ochronie danych osobowych, oraz
   2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
3. Poziom, co najmniej podwyższony stosuje się, gdy:
   1) w systemie informatycznym są przetwarzane dane, o których mowa w art. 27 ustawy o ochronie danych osobowych, oraz
   2) żadne z urządzeń systemu informatycznego, służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych jest połączone z siecią publiczną.

§6

Realizację zamierzeń określonych w § 4 powinny zagwarantować następujące założenia:

1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych;
2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych;

3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do różnych poziomów zbiorów danych osobowych – stosownie do indywidualnego zakresu upoważnienia;

4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń;

5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;

6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;

7) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

ROZDZIAŁ II

Przydział uprawnień i identyfikatorów

§7

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie.
2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.
3. Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień. Postanowienia ust. 2 nie dotyczą użytkowników, którzy jako jedyni mają dostęp do danych przetwarzanych w systemie informatycznym oraz użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.
4. Informatyk zobowiązany jest do prowadzenia ewidencji przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do zbiorów danych oraz dokonywaniem zmian w zakresie przyznanych uprawnień.

§8

Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe powinien posiadać umiejętność bezpiecznej obsługi komputera i dobrą znajomość oprogramowania systemowego i operacyjnego, z którego będzie korzystał.

§9

1. Każdy użytkownik – przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe – podlega przeszkoleniu w zakresie:

   1) obsługi komputera, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będzie wykorzystywał,

   2) przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.

2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§10

1. Za organizację szkoleń o których mowa w § 9 odpowiedzialny jest Administrator Danych.
2. Szkolenia odbywają się na wniosek kierowników komórek organizacyjnych.

§11

Do uwierzytelniania użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika.

§12

Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

§13

1. Identyfikatory dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela informatyk lub inna osoba upoważniona przez Administratora Danych.
2. Identyfikator użytkownika nie podlega zmianie.
3. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

§14

1. Pierwsze hasło dla użytkownika ustala Informatyk przy wprowadzaniu identyfikatora użytkownika do systemu.
2. Hasła muszą odpowiadać następującym wymogom:
   1) Hasła składają się co najmniej z:
      a) dla poziomu bezpieczeństwa podstawowego 6 znaków,
      b) dla poziomu bezpieczeństwa podwyższonego i wysokiego 8 znaków, i powinny zawierać małe litery oraz cyfry lub znaki specjalne,
   2) nie mogą być zapisywane w systemie w postaci jawnej,
   3) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,
   4) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

§15

1. Po otrzymaniu pierwszego hasła użytkownik zobowiązany jest zalogować się do systemu i powinien zmienić hasło. Przy wpisywaniu hasło nie może być wyświetlane na ekranie
2. Hasło zmieniane jest nie rzadziej, niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.

§16

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

§17

1. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł Informatyka, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Administratora Danych.
2. Tryb przechowywania i udostępniania haseł Informatyka określa załącznik **nr 1** do Instrukcji.

ROZDZIAŁ III

Rejestrowanie i wyrejestrowywanie użytkowników

§18

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi osoba odpowiedzialna za sprawy personalne wyznaczona przez Administratora Danych zgodnie z określonym wzorem.
2. Ewidencja zawiera:
   1) imię i nazwisko użytkownika;
   2) datę nadania i ustania upoważnienia,;
   3) zakres upoważnienia;
   4) identyfikator użytkownika.

3. Postanowienia ust. 2 pkt 4) nie dotyczą użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.
4. Ewidencja użytkowników może być prowadzona w systemie informatycznym.

§19

Nośniki magnetyczne (optyczne), na których gromadzone są wykazy zawierające ewidencję użytkowników przechowywane są w wyznaczonych szafach lub sejfach, do których ma dostęp wyłącznie Informatyk lub osoba upoważniona przez Administratora Danych Osobowych.

§20

Zmiany dotyczące użytkownika, takie jak:

1) Zmiana imienia lub nazwiska;
2) Zmiana zakresu upoważnienia,;
3) podlegają niezwłocznemu odnotowaniu w ewidencji, o której mowa w §18 Instrukcji.

§21

1. Zmiany dotyczące użytkownika, takie jak:
   1) rozwiązanie umowy;
   2) utrata upoważnienia do przetwarzania danych osobowych;
   3) zmiana zakresu obowiązków służbowych skutkujące ustaniem upoważnienia,

   powodują wyrejestrowanie użytkownika przez Informatyka, w trybie natychmiastowym, z ewidencji, o której mowa w § 18 Instrukcji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.
2. Kierowcy komórek organizacyjnych oraz osoba odpowiedzialna za sprawy kadrowe w przypadku osób na samodzielnych stanowiskach odpowiadają za natychmiastowe zgłoszenie do Informatyka, użytkowników, którzy utracili uprawnienia do dostępu do

danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji użytkowników o której mowa w § 18 Instrukcji.

§22

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. Osoba prowadząca ewidencje, o której mowa w § 18 Instrukcji, obowiązana jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenia.

§23

Dane dotyczące osób, które zostały wykreślone z ewidencji osób upoważnionych do przetwarzania danych osobowych, z przyczyn, o których mowa w §21 ust. 1 Instrukcji, są gromadzone w postaci odrębnych zbiorów archiwalnych lub stosuje się odpowiednie ich oznaczenia.

ROZDZIAŁ IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§24

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

§25

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa.

§26

1. Rozpoczynając prace na komputerze użytkownik loguje się do systemu informatycznego.
2. Użytkownik wprowadza identyfikator i dokonuje uwierzytelnienia.
3. Jeśli system to umożliwia, po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
4. Informatyk ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną.

§27

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:

1) wylogować się z sytemu informatycznego lub;
2) poczekać, aż zaktywizuje się blokowany hasłem wygaszacz ekranu.

§28

Kończąc pracę należy :

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

ROZDZIAŁ V

Procedury tworzenia kopii zapasowych

§29

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
2. Kopie zapasowe określone w ust. 1 niniejszego paragrafu powinny być sporządzone regularne w okresach wyznaczonych w załączniku **nr 2** do Instrukcji.
3. Za prawidłowe sporządzenie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest Informatyk.
4. Odpowiada on także za sprawdzenie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.
5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§30

1. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych, o ile zostali do tego upoważnieni przez Informatyka.
2. Użytkownicy określeni w ust. 1 są odpowiedzialni za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie.

§31

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.
2. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje Informatyk w obecności Administratora Danych lub osoby przez niego wyznaczonej.
3. Z nośników magnetycznych i optycznych wielokrotnego użytku, np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy

usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.

4. Dane zawarte na nośnikach optycznych jednokrotnego użytku, np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VI

Przetwarzanie danych osobowych

§32

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, zwłaszcza tzw. „wrażliwe", o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:
   1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub
   2) stosowanie metod kryptograficznych, lub
   3) stosowanie odpowiednich zabezpieczeń fizycznych, lub
   4) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
3. Dane osobowe zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
4. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.

5. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
6. Szczegółowy opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce bezpieczeństwa.

§33

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji dokumentów.
2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§34

Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Administrator Danych.

§35

Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Administrator Danych lub osoba przez niego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:

1) datę dokonania likwidacji,
2) przedmiot likwidacji (nośnik, kartoteka),
3) przedział czasowy likwidowanych zbiorów danych osobowych,
4) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ VII

Zabezpieczenie systemu informatycznego

§36

System informatyczny zabezpiecza się przed:

1) działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
2) utratą danych spowodowaną:
   a) działaniem nieautoryzowanego oprogramowania,
   b) awarią zasilania lub zakłóceniami w sieci zasilającej.

§37

1. Informatyk odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny.
2. Nowe wersje oprogramowania instaluje wyłącznie Informatyk niezwłocznie po ich otrzymaniu lub osoba upoważniona przez Informatyka.
3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Administrator Danych lub osoba przez niego upoważniona.

§38

1. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.
2. Program antywirusowy należy instalować również na komputerach przenośnych.

§39

W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§40

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów instalacyjnych.
2. Na serwerach, w miarę możliwości technicznych, oprogramowanie antywirusowe powinno być aktywne cały czas.
3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomionego pliku.

§41

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.

§42

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka.
2. Informatyk usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Administratora Bezpieczeństwa Danych lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.

§43

W razie niemożności usunięcia wirusa, Informatyk za zgodą Administratora Danych lub osoby upoważnionej, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.

§44

1. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.
2. Prace określone w ust. 1 są wykonywane pod nadzorem Informatyka lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.

§45

1. Informatyk jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.
2. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i używanych nośnikach danych.

§46

1. Po usunięciu wirusa Informatyk sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.
2. Informatyk sporządza raport o wystąpieniu wirusa. Raport winien zawierać następujące informacje:
    1) nazwę wirusa;
    2) datę wykrycia wirusa;
    3) miejsce zainfekowania;
    4) źródło infekcji.
3. Raport, o którym mowa w ust. 2 przekazywany jest Administratorowi Danych lub osobie przez niego wyznaczonej wraz z wnioskami, stosownymi do zaistniałej sytuacji.

§47

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
    1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
    2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

3. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

§48

Informatyk prowadzi wykaz przypadków zainfekowanych komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

§49

Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkownika.

ROZDZIAŁ VIII

Wymagania dotyczące sprzętu i oprogramowania

§50

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.

§51

1. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
2. Siec komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewnić

bezpieczne wyłączenie systemu informatycznego po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.

3. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie napięcia przez minimum 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak alby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
4. Zasilaczem awaryjnym powinna być zabezpieczona, co najmniej jedna stacja robocza.

§52

1. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest Informatyk.
2. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
3. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, modemy itd.) powinny być w miarę możliwości technicznych, włączone do wydzielonej sieci energetycznej, zapewniającej odpowiednie uziemienie i zabezpieczenie przed przepięciami.
4. Gniazda zasilania sieci komputerowej powinny być odpowiednio oznakowane, zabezpieczone przed wyłączeniem do nich innych odbiorników lub wykonane w specjalnych standardzie.

§53

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
2. Dane osobowe przesyłane po łączach telekomunikacyjnych wewnątrz danej sieci powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.

3. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnątrz powinny być w miarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.

§54

Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

§55

Informatyk odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.

§56

1. Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
2. Ekrany monitorów, powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
3. Za spełnienie obowiązku określonego w ust. 2 odpowiadają użytkownicy i kierownicy komórek organizacyjnych.

§57

1. Informatyk jest odpowiedzialny za to, aby każdej osobie, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu;
   2) identyfikatora użytkownika wprowadzającego dane chyba, że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą;

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

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

Wymagania określone w niniejszym ustępie nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostepnienia go na piśmie.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.
5. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie:
    1) daty pierwszego wprowadzenia danych;
    2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do tego sytemu informatycznego i przetwarzanych w nim danych posiada jedna osoba.
6. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w ust. 1 pkt 3, 4 i 5 należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

ROZDZIAŁ IX

Procedury wykonywania przeglądów i konserwacji

§58

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje Informatyk.
2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami upoważnień i odpowiedzialności.
3. Informatyk w uzasadnionych przypadkach może opracować dla poszczególnych zasobów informatycznych szczegółowe procedury techniczno - eksploatacyjne, które stanowią podstawę do eksploatacji danego zasobu informatycznego w sposób odmienny od określonego w niniejszej Instrukcji.
4. Procedury określone w ust. 3 nie dotyczą użytkowników, dotyczą wyłącznie Informatyka i upoważnionych pracowników służby informatycznej oraz osób upoważnionych przez Administratora Danych, które realizują prace techniczne i administratorskie w stosunku do poszczególnych zasobów informatycznych.

§59

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Administratora Danych przez uprawnionych przedstawicieli tych firm pod nadzorem Informatyka lub upoważnionego użytkownika i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

§60

1.W przypadku, gdy zaistnieje potrzeba naprawy lub wymienny sprzętu komputerowego służącego do przetwarzania lub przechowywania danych osobowych należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.

2.Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić w sposób uniemożliwiający ich odczytanie.

§61

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Informatyk lub osoba wyznaczona przez Administratora Danych.

ROZDZIAŁ X

Postanowienia końcowe

§62

1. Kierownicy komórek organizacyjnych są zobowiązani zapoznać z treścią Instrukcji każdego użytkownika.
2. Użytkownik jest zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także zobowiązaniu się do ich przestrzegania.

§63.

1.W sprawach nieuregulowanych w niemniejszej Instrukcji mają zastosowanie przepisy

ustawy o ochronie danych osobowych oraz wydawanych na jej podstawie aktów wykonawczych.

2.Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji

……
(podpis Administratora Danych)

Załącznik nr 1
do Instrukcji zarządzania
systemem informatycznym

TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ INFORMATYKA

Ustala się następujący tryb postepowania z hasłami Informatyka:

1. Hasła Informatyka przechowywane są w formie pisemnej w zapieczętowanej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada wyłącznie Burmistrz i osoby przez niego upoważnione.
3. Hasła, o którym mowa w pkt. 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Hasła zmieniane są, co najmniej, co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inna, nieupoważniona osobę.
5. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w pkt 1 i 2.
6. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki do dokumentów.
7. Niszczenia, o którym mowa w pkt 6 dokonuje Informatyk w obecności Burmistrza lub osoby przez niego upoważnionej.
8. W sytuacjach awaryjnych zaistniałych pod nieobecność Informatyka lub w razie jego niedyspozycji Burmistrz udostępnia hasło osobie prze siebie wyznaczonej.

…….
(podpis Administratora Danych)

Załącznik nr 2
do Instrukcji zarządzania
systemem informatycznym

CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH

Ustala się następującą częstotliwość tworzenia kopii awaryjnych:

1. Kopie dobowe i tygodniowe, wykonywane przez Informatyka lub użytkowników obejmujące:
   a. serwery danych;
   b. dział finansowy.
2. Kopie miesięczne, wykonywane na nośnikach zewnętrznych – magnetycznych lub optycznych umieszczane w zapieczętowanych kopertach, deponowane przez informatyka w miejscu określonym w § 29 Instrukcji obejmujące:
   a. serwery danych;
   b. dział finansowy;
   c. stacje robocze.
3. Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych.
4. Niszczenie kopii awaryjnych należy wykonywać w sposób określony w Instrukcji.
5. W sytuacjach awaryjnych zaistniałych pod nieobecność Informatyka lub w razie jego niedyspozycji Burmistrz udostępnia kopie awaryjne osobie przez siebie wyznaczonej.

……
(podpis Administratora Danych)