Załącznik nr 1
do Zarządzenia nr 111/2017
z dnia 9 czerwca 2017 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY MICHAŁOWICE

ZATWIERDZAM

WÓJT GMINY MICHAŁOWICE

mgr inż. Krzysztof Grabka

(podpis Administratora Danych)

Opracował:

Marcin Walichnowski

Oznaczenie dokumentu: **IT-SZBI-02**	Wersja dokumentu: 2.0	Dokument obowiązuje od: .....

Spis treści

10) **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 kierownika jednostki który decyduje o celach i środkach przetwarzania danych osobowych;

11) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych, 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;

12) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę lub osoby zatrudnione przez kierownika jednostki upoważnione do realizacji zadań związanych z zarządzaniem systemem informatycznym;

13) **kierowniku komórki organizacyjnej** – pojęcie obejmuje również samodzielne stanowisko pracy,

14) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez kierownika jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który został zaznajomiony ze stosownymi przepisami prawa oraz dokumentami wewnętrznymi dotyczącymi ochrony tych danych;

15) **zgodzie osoby, której 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) **ustawie** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.);

17) **Polityce** – rozumie się przez to niniejszy dokument;

18) **Instrukcji** – rozumie się przez to „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Michałowice" opracowaną na podstawie przepisów ustawy i rozporządzenia.

19) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – rozumie się przez to zbiór procedur i instrukcji mających na celu utrzymanie podstawowych atrybutów bezpieczeństwa systemu przetwarzania informacji, w szczególności poufności, dostępności i integralności informacji (wymienionych w Zarządzeniu Wójta Nr .....).

§ 11.

1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych posiadają dostęp jedynie osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik nr 2 do niniejszej polityki.
2. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla poszczególnych komórek organizacyjnych Urzędu.
3. Upoważnienia określone w ust. 1 przechowywane są w aktach osobowych pracownika.
4. Ewidencję osób biorących udział w przetwarzaniu danych osobowych prowadzi stanowisko do spraw kadrowo administracyjnych.
5. Wzór ewidencji określonej w ust. 4 stanowi załącznik nr 3 do Polityki bezpieczeństwa.

§ 12.

1. Wnioski o nadanie stosownych uprawnień (zgodnych z zakresem obowiązków) do systemów informatycznych (w tym służących do przetwarzania danych osobowych) przedkładają ASI lub Kierownikowi Referatu Informatyki, kierownicy komórek organizacyjnych lub osoby obejmujące samodzielne stanowiska.
2. Wypełnianie wniosków o których mowa w ust. 1 odbywa się na podstawie procedury „nadawania, modyfikacji, odebrania uprawnień do zasobów informatycznych" oznaczenie dokumentu: IT-SZBI-07.07 będącego częścią Systemu Zarządzania Bezpieczeństwem Informacji.
3. Ogólny wzór wniosku o nadanie stosownych uprawnień do systemów informatycznych stanowi dokument oznaczony: IT-SZBI-07.07a będący częścią Systemu Zarządzania Bezpieczeństwem Informacji.
4. Dostęp do zbirów danych przetwarzanych wyłącznie w formie papierowej lub papierowej wspomaganej przy użyciu oprogramowania biurowego dokumentuje się na Wnioskach o nadanie uprawnień dostępu do zbiorów danych osobowych (wzór wniosku stanowi załącznik nr 4 do niniejszej Polityki).
5. Wniosek o który mowa w punkcie 4 sporządzany jest przez Kierownika komórki organizacyjnej lub osobę zajmującą samodzielne stanowisko i przedkładany jest Kierownikowi Referatu Informatyki

§ 13.

1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w Urzędzie dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.
2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione środkami technicznymi adekwatnymi do kategorii danych oraz występujących zagrożeń.

4) doradztwo użytkownikom w zakresie bezpieczeństwa;

5) dbanie, aby dostęp do systemu posiadali użytkownicy mający stosowne zezwolenia oraz przeszkoleni w zakresie stosowania obowiązujących procedur bezpieczeństwa;

6) prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych,

§ 17.

1. Administrator Danych Osobowych wyznacza Administratorów Systemu Informatycznego, którzy posiadają najwyższe uprawnienia w systemie informatycznym. Tylko ASI są osobami uprawnionymi do instalowania i usuwania oprogramowania systemowego oraz 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, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.

3. Do zakresu odpowiedzialności i obowiązków Administratora Systemu Informatycznego należy:

   1) zapewnianie stałej sprawności urządzeń mających wpływ na bezpieczeństwo danych;

   2) odpowiadanie za bezpieczeństwo systemu informatycznego;

   3) zobowiązywanie i bieżąca kontrola stosowania się użytkowników do obowiązujących procedur;

   4) utrzymywanie i aktualizowanie kont użytkowników systemu informatycznego;

   5) zapewnianie aktualizacji dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności;

   6) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;

   7) wykonywanie kopii awaryjnych/archiwalnych oraz nadzór nad ich przechowywaniem;

   8) wprowadzanie i nadzór nad mechanizmami autoryzacji.

§ 18.

Kierownik komórki organizacyjnej (lub osoba zajmująca samodzielne stanowisko) 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, ze szczególnym uwzględnieniem zbiorów tradycyjnych (papierowych);

2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie;

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.

§ 22.

Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na rodzaj gromadzonych danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 tejże ustawy.

Rozdział IV
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 23.

1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , winien odbywać się 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.

3. Bezwzględnie zabronione jest podłączanie urządzeń (w szczególności komputerów) innych niż służbowe do sieci wewnętrznej Urzędu bez zgody i wiedzy ASI

4. Bezwzględnie zabronione jest podłączanie do komputerów w sieci wewnętrznej urządzeń (takich jak modemy GPRS, 3G, LTE itp.) nawiązujących połączenia do sieci zewnętrznych (np. Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi, WiMAX itp.).

§ 24.

Systemy dziedzinowe, przetwarzające dane osobowe mogą wymieniać się zgromadzonymi danymi, z zachowaniem zasad przetwarzania danych opisanych w ustawie, sposób połączeń i przepływu danych opisuje załącznik nr 7

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) 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, również danych niezbędnych administratorowi do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnych dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratora danych albo odbiorców danych, jeśli 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 art.32 ust. 1 pkt 1-5 ustawy, nie częściej niż raz na 6 miesięcy.

§ 28.

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 administratora danych.

§ 29.

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

4. Surowo zabronione jest pozostawianie jakichkolwiek wydruków w pomieszczeniach ogólnodostępnych bez nadzoru (np. „*ksero*", korytarze, pomieszczenia socjalne), niedopełnienie tego obowiązku uważa się za ciężkie naruszenie obowiązków pracowniczych.

§ 35.

Pomieszczenia, w których znajdują się akta lub systemy służące do przetwarzania danych osobowych winny być:

1) wyposażone w szafy zamykane na klucz umożliwiające przechowywanie dokumentów, w sposób zabezpieczający przed dostępem osób nieposiadających stosownych upoważnień,
2) zamknięte, jeśli nikt w nich nie przebywa.

§ 36.

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 IX
BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 37.

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.

§ 38.

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 i zgody kierownika komórki organizacyjnej oraz ASI.

§ 39.

Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 40.

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 (podejrzenie ujawnienia hasła), osoba przetwarzającej dane powinna niezwłocznie dokonać zmiany hasła.

wycofania z eksploatacji nośników komputerowych będącej częścią SZBI – oznaczenie dokumentu: IT-SZBI-07.04).

Dział XI
PLANY AWARYJNE I ZAPOBIEGAWCZE

§ 46.

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), znacząco obniży ryzyko awarii systemu w przypadku awarii zasilania.

§ 47.

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, automatycznej archiwizacji. Kopie archiwalne danych są wykonywane na nośnikach danych lub w magazynach dyskowych. Użycie kopii zapasowych następuje w przypadku odtwarzania systemu po awarii.

§ 48.

Administrator Systemu Informatycznego okresowo kontroluje poprawność kopii zapasowych oraz przydatność do odtworzenia systemu po awarii.

§ 49.

W przypadku wykrycia problemów z odtworzeniem danych z kopi zapasowej ASI niezwłocznie zawiadamia ABI o wykrytym problemie w celu opracowania nowych procedur wykonywania kopii zapasowych, uwzględniających rozwiązanie wykrytego problemu.

Rozdział XII
POLITYKA ANTYWIRUSOWA

§ 50.

1. Wszystkie 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) zabrania się instalowania oprogramowania typu „freeware" lub „shareware" oraz nieznanego pochodzenia bez zgody i wiedzy Administratora Systemu Informatycznego;
   3) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.
3. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku

Załącznik nr 1
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice"*

Reguły, dnia .....
(miejscowość, data)

_____
(imię i nazwisko)

OŚWIADCZENIE

Oświadczam, iż zostałem(am) zaznajomiony(a) z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych *„Polityką bezpieczeństwa przetwarzania danych osobowych"* oraz *„Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"*.

Oświadczam, iż zostałem(am) zaznajomiony(a) z dokumentacją *„Polityki Bezpieczeństwa Informacji"*.

Jednocześnie zobowiązuję się do ich przestrzegania.

(podpis osoby składającej oświadczenie)

Załącznik nr 2
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice”*

Reguły, dnia ……
(miejscowość, data)

_____
(imię i nazwisko)

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.), upoważniam Pana/Panią do przetwarzania danych osobowych.

Upoważnienie obejmuje prawo:
wglądu, wprowadzania, modyfikowania i usuwania danych osobowych. [1)]

Zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych *„Polityki bezpieczeństwa przetwarzania danych osobowych”* oraz *„Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”*.

(podpis Administratora Danych)

1) *Niepotrzebne skreślić*

Załącznik nr 3
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice"*

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

L.p.	Imię i nazwisko (1)	Data nadania upoważnienia (2)	Data ustania upoważnienia (3)	Zakres upoważnienia (4)	Login/identyfikator – system (lub oznaczenie karty nadania uprawnień zawierającej login lub identyfikator)	Uwagi/podpis ASI

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

.....
(podpis prowadzącego ewidencję w zakresie kol. 1-4)

Załącznik nr 4
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice"*

Reguły, dnia ……
(miejscowość, data)

Wniosek o nadanie uprawnień dostępu do zbiorów danych osobowych

Wnioskuję o nadanie Panu/Pani ……
dostępu do zbiorów danych osobowych zgromadzonych w systemach informatycznych Urzędu Gminy Michałowice zgodnie z poniższą listą określającą rodzaj udostępnianego zbioru oraz zakres dostępu:

Nazwa zbioru	**Nr zgł. W GIODO**	**Zakres dostępu *(d,w,m,u)*[1)]**
EWIDENCJA ARCHITEKTURY I BUDOWNICTWA	002228/1999	
EWIDENCJA ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH	005783/2009	
SKARGI I WNIOSKI	005785/2009	
SOŁTYSI	005786/2009	
SPRAWY DOTYCZĄCE ZAJĘCIA PASA DROGOWEGO	005787/2009	
OŚWIADCZENIA MAJĄTKOWE RADNYCH	005788/2009	
OCHRONA ŚRODOWISKA	005789/2009	
WNIOSKI O UDOSTĘPNIENIE INFORMACJI PUBLICZNEJ	005790/2009	
Program instalacji kolektorów słonecznych	005837/2010	
KANDYDACI NA ŁAWNIKÓW	007945/2011	
Konsultacje społeczne z mieszkańcami	004118/2012	
(nazwa zbioru zgłoszonego do GIODO)		

Oświadczam, że zakres dostępu zgodny jest z zakresem obowiązków osoby której wniosek dotyczy.

1) ***(d - wgląd; w - wprowadzanie; m - modyfikacja; u - usuwanie.)***

Zobowiązuję się od organizacji stanowiska pracy służącego do dostępu do wymienionych zbiorów, umożliwiającego przestrzeganie przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych *„Polityki bezpieczeństwa przetwarzania danych osobowych"* oraz *„Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"*.

(podpis kierownika komórki organizacyjnej lub osoby obejmującej samodzielne stanowisko)

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. (poz. 1536)

WZÓR

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

* ☐ — zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.),
* ☐ — zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
* ☐ — zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr .....
(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

.....

do Rejestru Zbiorów Danych Osobowych.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych): .....
.....
.....
.....
(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:
.....
.....
(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:
   * ☐ — administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),
   * ☐ — administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

   W przypadku powierzenia przetwarzania danych innemu podmiotowi, należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:
.....
.....
..... * ☐ *ew. cd. w załączniku nr* .....

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:
   * ☐ — zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,
   * ☐ — przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa —
.....
.....
..... * ☐ *ew. cd. w załączniku nr* .....

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:

*☐ — osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,

*☐ — przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych — *w przypadku odpowiedzi twierdzącej, należy podać odniesienie do przepisu tej ustawy:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

*☐ — przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

*☐ — przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych — *w przypadku odpowiedzi twierdzącej, należy podać, jakich:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

*☐ — przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

*☐ — przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

*☐ — przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

*☐ — przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

*☐ — przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,

*☐ — przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

11. Dane do zbioru będą zbierane:

*☐ — od osób, których dotyczą,

*☐ — z innych źródeł niż osoba, której dane dotyczą.

12. Dane ze zbioru będą udostępniane:

*☐ — podmiotom innym niż upoważnione na podstawie przepisów prawa.

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane — *należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania odbiorcy danych:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego — *należy podać nazwę państwa:*

.....

.....

..... *☐ *ew. cd. w załączniku nr* .....

Załącznik nr 6
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice"*

Zestawienie zbiorów danych osobowych oraz programów przeznaczonych do przetwarzania danych osobowych w Urzędzie Gminy Michałowice

Nazwa zbioru	**Nr zgł. W GIODO**	**Forma prowadzenia rejestru, nazwy systemów/programów posiadających dostęp do zbioru**
EWIDENCJA LUDNOŚCI	002226/1999 Nr księgi: 006989	**zbiór elektroniczny** SELWIN – System Ewidencji Ludności RWWIN – Rejestr Wyborców BAZA POSESJI – Przeglądarka bazy ewidencji ludności
EWIDENCJA GRUNTÓW	002227/1999 Nr księgi: 006990	**zbiór elektroniczny** EWOPIS – przeglądarka ewidencji gruntów
EWIDENCJA ARCHITEKTURY I BUDOWNICTWA	002228/1999 Nr księgi: 006996	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych**
EWIDENCJA NALEŻNOŚCI PODATKOWYCH	002229/1999 Nr księgi: 006995	**zbiór elektroniczny** System URZAD System URZADNT System Księgowo-Podatkowy U.I. INFO-SYSTEM
REJESTR KORESPONDENCJI	005782/2009 Nr księgi: 082214	**zbiór elektroniczny** System KANCELARIA-BIP System EZD
EWIDENCJA ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH	005783/2009 Nr księgi: 082235	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych**
NUMERACJA PORZĄDKOWA NIERUCHOMOŚCI	005784/2009 Nr księgi:082233	**zbiór elektroniczny** iMPA – Internetowy Menadżer Punktów Adresowych
SKARGI I WNIOSKI	005785/2009 Nr księgi: 082220	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych**
SOŁTYSI	005786/2009 Nr księgi: 082219	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych**

Nazwa zbioru	Nr zgł. W GIODO	Forma prowadzenia rejestru, nazwy systemów/programów posiadających dostęp do zbioru
Program instalacji kolektorów słonecznych	IT.142.4.2016	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych**
Biuletyn elektroniczny (newsletter)	IT.142.6.2015	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych** System CMS w domenie michalowice.pl
OPŁATY ZA WODĘ I ŚCIEKI	IT.142.2.2016	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych oraz w wybranym zakresie w formie elektronicznej** Zintegrowany system WODA MILLENNIUM - System rozliczania opłat wodno-kanalizacyjnych oraz opłat za gospodarowanie odpadami
Ewidencja usług dotyczących odbioru odpadów komunalnych	IT.142.1.2016	**zbiór prowadzony w formie tradycyjnej przy użyciu aplikacji biurowych oraz w wybranym zakresie w formie elektronicznej** Zintegrowany system WODA MILLENNIUM - System rozliczania opłat wodno-kanalizacyjnych oraz opłat za gospodarowanie odpadami

Załącznik nr 7
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice"*

Opis wymiany danych pomiędzy elektronicznymi systemami dziedzinowymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Michałowice

Nazwa zbioru udostępniającego dane	**Nazwa systemu/programu pobierającego dane oraz sposób wymiany danych**
EWIDENCJA LUDNOŚCI (baza programu SELWIN)	RWWIN – podgląd/odczyt danych CBP – podgląd/odczyt danych URZADNT - podgląd/odczyt danych

Załącznik nr 8
do „*Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice*"

Obszar przetwarzania danych osobowych w Urzędzie Gminy Michałowice

Obszar przetwarzania danych osobowych Urzędu Gminy Michałowice znajduje się w budynku:

w Regułach, ul. Aleja Powstańców Warszawy 1 obejmuje poniższy wykaz pomieszczeń:

PARTER
sala obsługi mieszkańców (pomieszczenie nr 1) – stanowiska biurowe/obsługi,
pok. 4,4a,– pomieszczenia biurowe,
pok. 5 – podręczne archiwum,
pok. 14. – kasa,
pok. 21 – archiwum,
pok. 19 – serwerownia,

I PIĘTRO
pok. 103 – pomieszczenie biurowe,
pok. 104 – pomieszczenie biurowe,
pok. 105 – pomieszczenie biurowe,
pok. 106 – pomieszczenie biurowe,
pok. 107 – pomieszczenie biurowe,
pok. 108 – pomieszczenie biurowe,
pok. 109 – pomieszczenie biurowe,
pok. 110 – pomieszczenie biurowe,
pok. 111 – pomieszczenie biurowe,
pok. 112 – pomieszczenie biurowe,
pok. 113 – pomieszczenie biurowe,
pok. 114 – pomieszczenie biurowe,
pok. 115 – pomieszczenie biurowe,
pok. 116 – pomieszczenie biurowe,
pok. 121 – pomieszczenie ksero,
pok. 122 – serwerownia,
pok. 123 – pomieszczenie biurowe,
pok. 126 – pomieszczenie biurowe,
pok. 128 – pomieszczenie biurowe,
pok. 129 – sala spotkań,

II PIĘTRO
pok. 201 – pomieszczenie biurowe,
pok. 202 – pomieszczenie biurowe,
pok. 203 – pomieszczenie biurowe,
pok. 204 – pomieszczenie biurowe,
pok. 205 – pomieszczenie biurowe,
pok. 206 – pomieszczenie biurowe,
pok. 207 – pomieszczenie biurowe,
pok. 208 – pomieszczenie biurowe,
pok. 209 – pomieszczenie biurowe,
pok. 210 – pomieszczenie biurowe,
pok. 211 – pomieszczenie biurowe,
pok. 212 – pomieszczenie biurowe,
pok. 213 – pomieszczenie biurowe,
pok. 214 – pomieszczenie biurowe,
pok. 216 – sala spotkań/konferencyjna,
pok. 218 – pomieszczenie ksero,
pok. 220 – sala spotkań/konferencyjna,
pok. 221 – sala spotkań,
pok. 226 – pomieszczenie biurowe

Przetwarzanie danych osobowych jest zabronione jeśli nie są spełnione warunki zdefiniowane w niniejszej Polityce.

Załącznik nr 9
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice"*

Struktura zbiorów danych osobowych przetwarzanych w formie elektronicznej

Szczegółowy opis struktury zbiorów danych osobowych wraz ze wskazaniem poszczególnych pól informacyjnych oraz powiązań między nimi znajduje się w dokumentacji technicznej będącej w posiadaniu autorów oprogramowania.

Nazwa zbioru	**Nr zgł. W GIODO**	**Autor oprogramowania, bazy danych, dokumentacji**
EWIDENCJA LUDNOŚCI	002226/1999 Nr księgi: 006989	SELWIN – System Ewidencji Ludności RWWIN – Rejestr Wyborców **ARAM Software sp. z o.o.,** **al. Jerozolimskie 200 lok. 236,** **02-486 Warszawa** **KRS: 0000588087, REGON: 363060854, NIP: 1182115317**
EWIDENCJA GRUNTÓW	002227/1999 Nr księgi: 006990	EWOPIS (wer. dla Gmin) – przeglądarka ewidencji gruntów **GEOBID spółka z o.o.** **40-844 Katowice, ul. Kossutha 11** **41-500 Chorzów, ul. Urbanowicza 37** **KRS: 0000060944, REGON: 271100591, NIP: 634-013-27-84**
EWIDENCJA NALEŻNOŚCI PODATKOWYCH	002229/1999 Nr księgi: 006995	System URZADNT **Sputnik Software Sp. z o.o.** **ul. Górecka 30** **60-201 Poznań** **KRS: 0000204111, REGON: 634582244, NIP: 7792230149** System Księgowo-Podatkowy U.I. INFO-SYSTEM **INFO-SYSTEM Roman i Tadeusz Groszek sp.j.** **ul. Marszałka Józefa Piłsudskiego 31 lok. 240** **05-120 Legionowo** **REGON: 015 664 091, NIP: 536 174 53 79**

Nazwa zbioru	Nr zgł. W GIODO	Autor oprogramowania, bazy danych, dokumentacji
OPŁATY ZA WODĘ I ŚCIEKI	IT.142.2.2016	Zintegrowany system WODA MILLENNIUM - System rozliczania opłat wodno-kanalizacyjnych oraz opłat za gospodarowanie odpadami **Firma Alti** **ul. Mikołaja Reja 4** **83-330 Żukowo**
Ewidencja usług dotyczących odbioru odpadów komunalnych	IT.142.1.2016	Zintegrowany system WODA MILLENNIUM - System rozliczania opłat wodno-kanalizacyjnych oraz opłat za gospodarowanie odpadami **Firma Alti** **ul. Mikołaja Reja 4** **83-330 Żukowo**

Załącznik nr 2
do Zarządzenia nr ..111/2017...
z dnia..9 czerwca 2017r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY MICHAŁOWICE

ZATWIERDZAM
WÓJT GMINY MICHAŁOWICE
---
mgr inż. Krzysztof Grabka
(podpis Administratora Danych)

Opracował:

Marcin Walichnowski

Oznaczenie dokumentu: **IT-SZBI-03**	Wersja dokumentu: 2.0	Dokument obowiązuje od: .....

Rejestr zmian dokumentu:

Lp	Imię i nazwisko wprowadzającego zmiany	Wersja	Data	Opis/Uwagi
1	Marcin Walichnowski	1.0	2014-08-25	Opracowanie dokumentu.
2	Marcin Walichnowski	2.0	……..	Przegląd dokumentu i dopasowanie do Systemu Zarządzania Bezpieczeństwem Informacji

Niniejsza „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zwana dalej Instrukcją została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.) 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).

§ 1.

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy Michałowice, określa:

1) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
2) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
3) zasady i procedury rozpoczynania i kończenia pracy,
4) zasady i częstotliwość tworzenia kopii bezpieczeństwa,
5) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,
6) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
7) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
8) zasady postępowania w zakresie komunikacji w sieci komputerowej.

§ 2.

Ilekroć w Instrukcji jest mowa o:

1) **ustawie** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.), zwaną dalej „ustawą";
2) **rozporządzeniu** - rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)
3) **Jednostce (Urzędzie)** - rozumie się przez to Urząd Gminy Michałowice;
4) **kierowniku komórki organizacyjnej** – pojęcie obejmuje również samodzielne stanowisko pracy;
5) **identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

6) **haśle** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

7) **sieci lub sieci telekomunikacyjnej** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, ze zm.);

8) **sieci publicznej** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, ze zm.);

9) **integralności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

10) **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

11) **uwierzytelnianiu** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

12) **Administratorze Danych (AD)** - w świetle przepisów ustawy o ochronie danych osobowych , art. 3 i 7 pkt 4 rozumie się przez to Wójta Gminy, który decyduje o celach i środkach przetwarzania danych osobowych;

13) **Administratorze Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych (kierownika jednostki), 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;

14) **Administratorze Systemu Informatycznego (ASI)**, zwanego też **Administratorem** Systemu - rozumie się przez to osobę lub osoby zatrudnione przez kierownika jednostki, upoważnione do realizacji zadań związanych z zarządzaniem systemem informatycznym;

15) **użytkowniku systemu informatycznego** - rozumie się przez to upoważnioną przez kierownika jednostki, pracownika do przetwarzania danych osobowych w systemie informatycznym, który odbył stosowne szkolenie w zakresie ochrony danych.

16) **Instrukcji** – rozumie się przez to niniejszy dokument.

17) **Polityce** – rozumie się przez to „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice" opracowaną na podstawie przepisów ustawy i rozporządzenia.

18) **Systemie Zarządzania Bezpieczeństwem Informacji (SZBI)** – rozumie się przez to zbiór procedur i instrukcji mających na celu utrzymanie podstawowych atrybutów bezpieczeństwa systemu przetwarzania informacji, w szczególności poufności, dostępności i integralności informacji (wymienionych w Zarządzeniu Wójta Nr .....).

§ 3.

Procedury nadawania uprawnień:

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) upoważniona do dostępu do systemu przez Administratora Danych na wniosek kierownika komórki organizacyjnej. W przypadku osób zatrudnionych na samodzielnych stanowiskach osoba taka wnioskuje o nadanie sobie uprawnień zgodnie ze swoim zakresem obowiązków oraz nadanym upoważnieniem.

2. Rejestracja, o której mowa w ust. 1, polega na nadaniu przez ASI identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

3. Szczegółowe czynności związane z przydzielaniem uprawnień opisuje procedura nadawania, modyfikacji i odebrania uprawnień do zasobów informatycznych stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.07.

§ 4.

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje ASI na wniosek kierownika komórki organizacyjnej.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

   1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),

   2) usunięcie danych dostępowych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

   1) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,

   2) zawieszenie w pełnieniu obowiązków służbowych,

   3) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

6. Wniosek o którym mowa w ust. 1 powinien mieć formę pisemną, wzór wniosku stanowi załącznik nr 1 do Instrukcji

7. Szczegółowe czynności związane z wyrejestrowaniem uprawnień opisuje procedura nadawania, modyfikacji i odebrania uprawnień do zasobów informatycznych stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.07.

§ 5.

1. Zgodnie z Rozporządzeniem ustala się zasady postępowania z hasłami dostępu.

2. Szczegółowe zasady postępowania z hasłami opisuje procedura tworzenia i zarządzania hasłami stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.11

3. Szczegółowe zasady postępowania z hasłami administracyjnymi opisuje procedura przechowywania i udostępniania haseł administracyjnych stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.09

§ 6.

Rozpoczęcie pracy w systemie odbywa się poprzez:

1) przygotowanie stanowiska pracy,

2) włączenie stacji roboczej,

3) wprowadzenie swojego identyfikatora i hasła, przy czym wprowadzenie hasła odbywa się w sposób uniemożliwiający jego podejrzenie.

4) Szczegółowe zasady postępowania opisuje procedura rozpoczęcia, zawieszenia i zakończenia pracy stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.08

§ 7.

Opuszczenie stanowiska pracy odbywa się po uprzednim:

1) zabezpieczeniu dokumentacji przed dostępem osób postronnych,

2) wylogowaniem użytkownika z systemu,

3) zablokowaniem dostępu do komputera (przełączenie komputera w tryb wymagający podania hasła).

4) Szczegółowe zasady postępowania opisuje procedura rozpoczęcia, zawieszenia i zakończenia pracy stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.08

§ 8.

Zakończenie pracy w systemie odbywa się poprzez:

1) zamknięcie aplikacji,

2) zamknięcie systemu operacyjnego,

3) wyłączenie stacji roboczej,

4) zabezpieczeniem stanowiska pracy przed dostępem osób nieupoważnionych.

5) Szczegółowe zasady postępowania opisuje procedura rozpoczęcia, zawieszenia i zakończenia pracy stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.08

§ 9.

Zabrania się użytkownikom pracującym w systemie:

1) udostępniania stacji roboczej osobom postronnym z zastrzeżeniem pkt 2),

2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z ASI,

3) używania nielicencjonowanego oprogramowania.

§ 10.

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do ASI, a w szczególności:

   1) naruszenia bezpieczeństwa systemu informatycznego,

   2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. ASI zgłasza w szczególności przypadki:

   1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,

   2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,

   3) usuwania, dodawania lub modyfikowania baz wiedzy i zgody użytkownika jego dokumentów (rekordów),

   4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

   5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,

   6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,

   7) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem ASI jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. Użytkownik sieci i ASI w porozumieniu z Kierownikiem Referatu Informatyki ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 11.

1. Kopie zapasowe zbiorów danych osobowych tworzone są w ramach całego systemu teleinformatycznego.
2. Częstotliwość, sposób tworzenia oraz miejsce przechowywania kopii zapasowych reguluje procedura tworzenia i przechowywania kopii zapasowych stanowiąca część Systemu Zarządzania Bezpieczeństwem Informacji – oznaczenie dokumentu IT-SZBI-07.03

§ 12.

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz stacjami roboczymi.
3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, ASI kontroluje nie rzadziej niż raz na kwartał prawidłowość funkcjonowania systemu antywirusowego.
4. Do obowiązków ASI należy zapewnienie prawidłowej aktualizacji oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

§ 13.

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych (np. utratą integralności danych) spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).

§ 14.

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, lub likwidacji dopiero po uprzednim uzyskaniu zgody ASI.
2. Urządzenia, o których mowa w ust. 1 przed ich przekazaniem pozbawia się zapisanych danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.
3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.
4. Jeżeli nie jest możliwe pewne pozbawienie urządzenia przekazywanego do likwidacji zapisanych danych osobowych, urządzenie - przed przekazaniem - uszkadza się fizycznie w sposób uniemożliwiający odczytanie tych danych.

§ 15.

1. Przeglądu i konserwacji systemu dokonuje ASI doraźnie.
2. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik doraźnie, o podejrzeniu zaistniałych nieprawidłowości niezwłocznie zawiadamia ASI.

§ 16.

1. Operacje wykonywane w systemach teleinformatycznych Urzędu Gminy Michałowice zgodnie z par.21 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 526 ze zm.) podlegają wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach)
2. W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:
   1) systemu z uprawnieniami administracyjnymi;
   2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
   3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
3. Poza informacjami wymienionymi w ust. 2 na podstawie decyzji ASI mogą być odnotowywane również inne działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:
   1) działań użytkowników nieposiadających uprawnień administracyjnych,
   2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
   3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny - w zakresie wynikającym z analizy ryzyka.
4. Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata
5. Zapisy dzienników systemów mogą być składowane na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji.
6. W uzasadnionych przypadkach dzienniki systemów mogą być prowadzone na nośniku papierowym.

§ 17.

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe ASI zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, ASI powinien uwzględniać dedykowane przyzwolenia dostępu, tj. zapewnić kontrolę nad tym kto i w jaki sposób może uzyskać dostęp do zasobów sieciowych

§ 18.

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (sieć LAN) musi być zorganizowane w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu w porozumieniu z ASI wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 19.

1. Do przesyłania danych w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane wyłącznie kanały transmisji wykorzystywane przez autoryzowane programy lub systemy oraz wyłącznie w oparciu o przepisy prawne regulujące sposób udostępniania (przesyłania) tych danych poza obszar urzędu.

2. W przypadku braku przepisów o których mowa w ust.1 określających sposób przesłania danych użytkownik w porozumieniu z ASI powinien zapewnić środki kryptograficzne umożliwiające bezpieczne przesłanie informacji.

§ 20.

1. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

2. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

§ 21.

1. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

2. Ekrany monitorów wszystkich stanowisk są zaopatrzone w wygaszacze z ustawioną opcją *„wymagania hasła”*, które po upływie maksymalnie 15 minut nieaktywności użytkownika automatycznie wyłączają możliwość podglądu ekranu, oraz żądają ponownej autoryzacji dostępu do komputera.

§ 22.

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§ 23.

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nieposiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.

2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 24.

Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji. Niniejszy dokument jest częścią Systemu Zarządzania Bezpieczeństwem Informacji, w wypadku odrębnych od zawartych w niniejszej Instrukcji uregulowań występujących w pozostałych politykach, procedurach i instrukcjach należących do SZBI lub innych procedurach obowiązujących w Jednostce, użytkownicy mają obowiązek stosowania unormowań dalej idących (bardziej restrykcyjnych), których stosowanie zapewni wyższy poziom ochrony danych osobowych.

§ 25.

Niniejszy dokument jest dokumentem wewnętrznym i nie może być udostępniany osobom postronnym w żadnej formie (art. 39 ust.2 Ustawy o ochronie danych osobowych).

Załącznik nr 1
do „*Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Michałowice*"

Reguły, dnia ……
(miejscowość, data)

Wniosek wyrejestrowanie użytkownika z systemów komputerowych

Wnioskuję o **czasowe**[1)] **/ trwałe**[1)] wyrejestrowanie

Pana/Pani ……

(imię nazwisko, stanowisko)

z systemów komputerowych umożliwiających dostęp do systemów informatycznych Urzędu Gminy Michałowice

Uwagi:

……

……

……

1) *Niepotrzebne skreślić*

(podpis kierownika komórki organizacyjnej lub stanowiska ds. kadr)