Zarządzenie Nr 62
Burmistrza Miasta i Gminy Ryn
z dnia 24 maja 2018r.

w sprawie „Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Miasta i Gminy w Rynie”

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2017 r. poz. 1875 i 2232, z 2018 r. poz. 130) oraz Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018r, poz. 1000), zarządzam, co następuje:

§ 1.

Ustalam :

1) „Politykę bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Miasta i Gminy w Rynie” - stanowiącą załącznik Nr 1 do zarządzenia,
2) „Instrukcję zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Rynie” - stanowiącą załącznik Nr 2 do zarządzenia.

§ 2.

Wykonanie Zarządzenia powierzam Sekretarzowi Gminy Ryn.

§ 3.

Traci moc Zarządzenie Nr 133 Burmistrza Miasta i Gminy Ryn z dnia 31 grudnia 2014r. w sprawie wprowadzenia „Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Miasta i Gminy w Rynie”

§ 4.

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Miasta i Gminy Ryn
Józef Karpiński

Załącznik Nr 1
do Zarządzenia Nr 62
Burmistrza Miasta i Gminy Ryn
z dnia 24.05.2018r.

POLITYKA BEZPIECZEŃSTWA

w zakresie ochrony danych osobowych

w Urzędzie Miasta i Gminy Ryn

Rozdział I

Częśćć ogólna

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych, zwana dalej Polityką Bezpieczeństwa określa sposób przetwarzania oraz zabezpieczania danych osobowych zgromadzonych w rejestrach prowadzonych w celu realizacji zadań ustawowych przez Urząd Miasta i Gminy w Rynie.

§ 2

Ze względu na wagę problemów związanych z ochroną prawa do prywatności, a w szczególności prawa osób fizycznych powierzających swoje dane osobowe, do właściwej i skutecznej ochrony tych danych należy:

1) podjąć wszelkie niezbędne działania w zakresie ochrony praw i usprawiedliwionych interesów jednostki związane z bezpieczeństwem danych osobowych,
2) podnosić świadomość oraz kwalifikacje osób przetwarzających dane osobowe w Urzędzie Miasta i Gminy w Rynie w zakresie problematyki bezpieczeństwa tych danych,
3) traktować obowiązki przy przetwarzaniu danych osobowych, przez osoby zatrudnione w Urzędzie Miasta i Gminy w Rynie, jako należące do kategorii podstawowych obowiązków pracowniczych,
4) stałe doskonalić i rozwijać nowoczesne metody przetwarzania danych oraz podejmować i rozwijać organizacyjne, techniczne i informatyczne środki ochrony tych danych tak, aby skutecznie zapobiegać zagrożeniom związanym z:
   a) nieautoryzowanym dostępem, wykradaniem bądź niszczeniem danych przez wszelkiego rodzaju mechanizmy i programy szpiegujące, wirusy komputerowe i inne niepożądane oprogramowanie,
   b) dostępem do nieautoryzowanych i niezabezpieczonych stron internetowych, mogących posiadać skrypty pozwalające wykradać zasoby komputera, który się z nimi łączy,
   c) atakami z sieci uniemożliwiającymi przetwarzanie danych (ataki typu DOS na serwery) oraz spamem,
   d) użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania danych poza Urząd,
   e) możliwością niekontrolowanego kopiowania danych na zewnętrzne, nośniki,
   f) działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
   g) lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez zabezpieczenia,
   h) brakiem świadomości niebezpieczeństwa przy dopuszczaniu osób postronnych do swojego stanowiska pracy,
   i) kradzieżą sprzętu lub nośników z danymi,
   j) kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
   k) przekazywaniem niezabezpieczonego sprzętu komputerowego do serwisu zewnętrznego

i innym zagrożeniom mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

Rozdział 2

Definicje

§ 3

Użyte w niniejszej Polityce sformułowania lub skróty oznaczają:

1) **Urząd -** Urząd Miasta i Gminy w Rynie;
2) **Burmistrz -** Burmistrza Miasta i Gminy Ryn;
3) **komórka organizacyjna -** wyodrębniony element struktury Urzędu realizujący zadania określone w niniejszym Regulaminie, w szczególności: referat lub samodzielne stanowisko;
4) **ADO -** Administratora Danych Osobowych, którym w UMiG Ryn jest Burmistrz;
5) **IOD -** osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Inspektora Ochrony Danych;
6) **ASI -** osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Systemu Informatycznego Urzędu;
7) **użytkownik danych** – każdy pracownik, który wykonując czynności służbowe, przetwarzający dane osobowe, tzn. wykonujący na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie;
8) **osoba upoważniona** – osoba posiadająca upoważnienie wydane przez administratora lub osobę uprawnioną przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu;
9) **osoba uprawniona –** osoba posiadająca upoważnienie wydane przez administratora do wykonywania w jego imieniu określonych czynności;
10) **sieć lokalna** – połączenie funkcjonujących w Urzędzie systemów informatycznych i stacji roboczych przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;
11) **stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie;
12) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, połączeń sieciowych i narzędzi programowych zastosowanych w celu przetwarzania danych;
13) **bezpieczeństwo systemu informatycznego** – wdrożone przez administratora lub osobę przez niego uprawnioną, środki organizacyjne i techniczne w celu zabezpieczenia oraz ochrony danych przed nieautoryzowanym dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem;
14) **przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
15) **system przetwarzania danych** – ta część systemu informatycznego oraz te procedury przetwarzania dokumentów papierowych, które razem tworzą system współpracujących ze sobą mechanizmów wykorzystywanych przy przetwarzaniu danych w Urzędzie;
16) **integralność danych** – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
17) **poufność danych** – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom i osobom;
18) **zbiór danych osobowych** – każdy posiadający strukturę logiczną zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

Rozdział 3

Cel wprowadzenia Polityki Bezpieczeństwa

§ 4

Celem wprowadzenia niniejszej Polityki Bezpieczeństwa jest:

1) ochrona danych osobowych przetwarzanych i gromadzonych w Urzędzie i dotyczy:
   a) zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
   b) metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
   c) procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
   d) ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
   e) określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny,
2) zmniejszenie ryzyka utraty informacji,
3) określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych,
4) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych danych.

Rozdział 4

Zakres stosowania Polityki Bezpieczeństwa

§ 5

Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych w tym do systemu informatycznego, a w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
2) informacji będących własnością Urzędu lub jednostek obsługiwanych, o ile zostały przekazane do Urzędu na podstawie umów lub porozumień ,
3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

Rozdział 5

Sposób i zakres udostępniania dokumentu.

§ 6

1. Z niniejszym dokumentem powinni zapoznać się wszyscy pracownicy administracyjni Urzędu, a w szczególności:
   1) osoby upoważnione do przetwarzania danych osobowych w zbiorach i bazach danych,
   2) obsługa informatyczna Urzędu,
2. Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników odpowiedzialny jest IOD.
3. Dokument powinien zostać umieszczony w formie elektronicznej, na wewnętrznych zasobach sieciowych, do których dostęp posiadają wszyscy pracownicy Urzędu lub w uzasadnionych przypadkach powinien zostać im przedłożony w formie papierowej.

Rozdział 6

Zasady ogólne

§ 7

W celu zabezpieczenia danych gromadzonych i przetwarzanych w Urzędzie oraz w celu podniesienia bezpieczeństwa w przetwarzających je systemach informatycznych, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady postępowania.

§ 8

Pracownicy Urzędu, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, dokładają szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewniają, aby dane te były:
- przetwarzane zgodnie z prawem,
- zbierane do oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 9

Polityka bezpieczeństwa odnosi się do danych osobowych przetwarzanych w zbiorach:
- tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
- w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

§ 10

Dane osobowe w Urzędzie przetwarzane są w celu:

- realizacji statutowych zadań i obowiązków,
- zapewnienia prawidłowej, zgodnej z prawem polityki personalnej i bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia nawiązywanych przez Urząd działający jako pracodawca w rozumieniu art. 3 kodeksu pracy,
- realizacji innych usprawiedliwionych celów i zadań Urzędu z poszanowaniem praw i wolności osób powierzających Urzędowi swoje dane.

§ 11

Wprowadzona zostaje następująca klasyfikacja informacji :

1. **Informacje niejawne** – informacje, których ujawnienie może spowodować istotne straty finansowe lub problemy prawne i co do których stosuje się przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych np.:
    1) dane osobowe petentów i zatrudnionych pracowników,
    2) dane o wynagrodzeniach i historii zatrudnienia pracowników,
2. **Informacje wewnętrzne** – wszystkie informacje wytworzone wewnątrz Urzędu, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji), nieprzeznaczone do przedstawienia na forum publicznym;
    1) Informacje **wewnętrzne dostępne** – informacje dostępne dla wszystkich pracowników Urzędu,
    2) Informacje **wewnętrzne zastrzeżone** – informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
    3) Informacje **stanowiące tajemnicę pracodawcy** – informacje, których upublicznienie może narazić Urząd na szkodę,
3. **Informacje publiczne/jawne** – informacje, które mogą być przedstawione na forum i do wiadomości publicznej;

Rozdział 7

Zapisy szczegółowe

§ 12

Polityka bezpieczeństwa została opracowana na podstawie: Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych

§ 13

Urząd przetwarza przedmiotowe dane z poszanowaniem obowiązujących w tym zakresie przepisów ustawy z dnia 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000); Rozporządzenia

Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE i ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

§ 14

Pod szczególną ochroną Urzędu pozostają dane osobowe wrażliwe wymienione w art. 9 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Rozdział 8

Wyznaczenie administratorów i ich obowiązki

§ 15

1. Osobą odpowiedzialną za właściwy i niezakłócony przebieg przetwarzania danych, w rozumieniu ustawy z dnia 10.05.2018r. o ochronie danych osobowych (Dz. U. z 2018r. poz. 1000), w systemach służących do przetwarzania danych osobowych jest Administrator Danych Osobowych.
2. W związku z powyższym do zadań **Administratora Danych Osobowych** należy:

1. Prawna odpowiedzialność za funkcjonowanie Urzędu, w tym również za przestrzeganie wymagań związanych z zabezpieczeniem informacji i systemu informatycznego;
2. Zatwierdzanie i publikowanie dokumentów związanych z ochroną informacji, dotyczących wszystkich lub znacznej grupy pracowników;
3. Zapewnienie wsparcia organizacyjno - finansowego przy wdrażaniu mechanizmów zabezpieczenia informacji i systemu informatycznego;
4. Zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do procesu przetwarzania i przechowywania danych osobowych;
5. Uwzględnianie kryterium wiarygodności zatrudnianych pracowników przy rekrutacji na stanowiska związane z dostępem do informacji krytycznych lub z administracją krytycznych komponentów informatycznych;
6. Zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych;
7. Zapewnienie pracownikom szkoleń w zakresie poszerzania wiedzy i świadomości związanej z bezpieczeństwem informacji oraz stosowanymi rozwiązaniami, używanymi w administracji publicznej w celu utrzymania bądź zapewnienia odpowiedniego poziomu zabezpieczeń stosowanych w procesach przetwarzania i gromadzenia danych;
8. Wyznaczenie Inspektora Danych Osobowych i Administratora Systemu Informatycznego.

§ 16

Wyznaczony zostaje **Inspektor Danych Osobowych**, do którego zadań należy:

1. Określanie wagi i znaczenia informacji gromadzonych i przetwarzanych w Urzędzie w celu realizacji jego zadań;
2. Koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych w Urzędzie, jego poszczególnych działach, sekcjach i samodzielnych stanowiskach;
3. Uwzględnienie prawnych aspektów w procesie zabezpieczenia przetwarzania danych z uwzględnieniem zabezpieczenia systemu informatycznego;
4. Akceptacja lub wyrażanie potrzeby obniżenia poziomu ryzyka związanego z przetwarzaniem informacji w Urzędzie;
5. Proponowanie sposobu realizacji mechanizmów ochrony danych z uwzględnieniem specyfiki pracy danej komórki organizacyjnej;
6. Określanie i nadzór nad wdrożeniem, standardów zabezpieczeń informacji w Urzędzie;
7. Opiniowanie wszelkich zmian zachodzących przy procesie przetwarzania danych pod kątem ich wpływu na bezpieczeństwo;
8. Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa systemu informatycznego i wyciąganie konsekwencji dyscyplinarnych wobec podległych sobie pracowników zamieszanych w tego typu incydenty;
9. Koordynacja procesu reakcji na incydenty w zakresie naruszenia bezpieczeństwa informacji ;
10. Koordynacja działań związanych z uświadomieniem pracownikom znaczenia ochrony informacji;

§ 17

Wyznaczony zostaje **Inspektor Danych Osobowych**, do którego zadań należy:

1. Implementacja odpowiednich mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej;
2. Merytoryczne przygotowanie i przeprowadzenie szkoleń w zakresie zachowania bezpieczeństwa przy przetwarzaniu danych;
3. Nadawanie uprawnień użytkownikom systemu informatycznego zgodnie z wnioskami ich przełożonych;
4. Zapewnienie podstawowego szkolenia w zakresie korzystania z systemu informatycznego nowo przyjętych pracowników;
5. Odbieranie uprawnień użytkownikom, u których zakończył się okres zatrudnienia;
6. Zapewnienie pomocy użytkownikom przy korzystaniu z systemu

informatycznego;

7. Tworzenie kopii zapasowych danych przechowywanych w systemie informatycznym;

8. Zarządzanie licencjami;

9. Monitorowanie poziomu bezpieczeństwa w systemie informatycznym, a w szczególności bieżącego stanu aktualizacji systemów operacyjnych i serwerów oraz sygnatur programów antywirusowych, rejestrowanie czynności przetwarzania danych osobowych;

10. Monitorowanie działania systemu informatycznego i przekazywanie informacji o zagrożeniach osobie IOD, a w przypadku jego nieobecności bezpośrednio osobie ADO;

11. Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwania ich skutków.

12. Zarządzanie określonymi rozwiązaniami technicznymi związanymi z ochroną systemu informatycznego;

13. Kontrolowanie przestrzegania zasad bezpiecznego przetwarzania danych w systemie informatycznym;

14. Czasowe przeglądy i weryfikacja m.in.:

1) ilości i wykazu pomieszczeń dopuszczonych do przetwarzania danych,

2) rozmieszczenia stacji roboczych w poszczególnych pomieszczeniach,

3) sprawności użytkowanego sprzętu,

4) legalności zainstalowanego oprogramowania,

5) poprawności instalacji łatek systemowych i aktualizacji sygnatur wirusów programu antywirusowego,

6) przyznanych uprawnień do baz danych;

7) weryfikacja harmonogramu logowania do systemu informatycznego dla poszczególnych użytkowników.

Rozdział 9

Zasady udzielania uprawnień do przetwarzania danych pracownikom Urzędu

§ 18

1. Dostęp pracowników do systemu informatycznego, programów przetwarzających dane osobowe oraz urządzeń z nimi powiązanych możliwy jest wyłącznie na podstawie upoważnienia wydanego przez ADO.

2. Wniosek o wydanie upoważnienia do przetwarzania danych, składany jest w formie pisemnej na wniosek przełożonego pracownika do ADO lub IOD.

3. Przed dopuszczeniem do pracy w systemie informatycznym, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą polityką bezpieczeństwa.

4. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.

5. Osoba przetwarzająca dane osobowe składa oświadczenie o zapoznaniu się z przepisami o odpowiedzialności karnej i dyscyplinarnej za naruszenie bezpieczeństwa danych osobowych oraz zachowaniu tajemnicy służbowej.

6. Oświadczenia o zachowaniu tajemnicy służbowej, przechowywane są w aktach osobowych pracowników.

7. Fakt zapoznania się z niniejszą Polityką, pracownik potwierdza własnoręcznym podpisem na stosownym wykazie.

Rozdział 10

Obowiązki pracowników w zakresie zachowania bezpieczeństwa przetwarzanych danych

§ 19

1. Każdy pracownik Urzędu powinien:

   1) Przestrzegać zasad zachowania bezpieczeństwa podczas pracy w systemie informatyczny

   2) W należyty sposób chronić przed niedozwolonymi zmianami, nieupoważnionym dostępem, rozpowszechnianiem, uszkodzeniem lub zniszczeniem wszelkiego rodzaju dokumentów księgowych m.in. takich jak:

      a) księgi rachunkowe,

      b) dowody księgowe,

      c) dokumenty inwentaryzacyjne,

      d) sprawozdania finansowe,

      e) przetwarzanych zarówno w formie elektronicznej jak i papierowej;

   3) Brać aktywny udział w szkoleniach dotyczących bezpieczeństwa informacji i systemu informatycznego;

   4) Informować o incydentach w zakresie bezpieczeństwa systemu informatycznego;

   5) Brać aktywny udział we wdrażaniu mechanizmów bezpieczeństwa poprzez opiniowanie możliwości zastosowania określonego rozwiązania przy realizacji zadań danego pracownika;

   6) Bezwzględnie wykonywać polecenia IOD, ASI w zakresie ochrony informacji

i bezpieczeństwa systemu informatycznego;

7) Po otrzymaniu indywidualnych identyfikatorów i haseł dostępu powinien je zapamiętać
i zachować w ścisłej tajemnicy;

2. Zabrania się:

1) Zapisywania identyfikatorów i haseł dostępu do systemu informatycznego i programów w miejscach, które umożliwiłyby osobom trzecim zapoznanie się z nimi;
2) Udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym;
3) Wykorzystywania komputerów i zasobów sieci teleinformatycznej w celach innych niż służbowe;
4) Samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji);
5) Trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie;
6) Publicznego rozpowszechniania programów komputerowych lub ich kopii;
7) Przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko;
8) Udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu;
9) Wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez wyraźnego upoważnienia administratora lub IOD;
10) Używania prywatnych skrzynek mailowych działających na innych serwerach niż urzędowy bez uzgodnienia z administratora lub IOD;
11) Uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści;
12) Kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody administratora lub IOD;

3. W szczególności w celu zwiększenia bezpieczeństwa danych i sieci komputerowej:

1) Ogranicza się w Urzędzie obieg dyskietek, pendrive-ów i innych nośników informatycznych poprzez ich oznaczenie i zarejestrowanie w ewidencji wewnętrznej Urzędu.

2) Wprowadza się zakaz obiegu nośników nie oznakowanych w sposób, o którym mowa w ust.1, a wszystkie nośniki pochodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu ich zawartości po uprzednim sprawdzeniu programem antywirusowym.

3) Każdy użytkownik ma obowiązek usunięcia danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych oraz do usuwania danych z nośników, które przeznaczone są do likwidacji.

4. Działania Pracodawcy zmierzające do poprawy jakości pracy w systemie informatycznym

Urzędu polegające w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążeniu sieci informatycznej poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnej treści oraz kontroli antywirusowej nie wymagają zgody pracownika.

Rozdział 11

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przy komputerze

§ 20

1. Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną.
2. Użytkownicy uzyskują bezpośredni dostęp do systemu informatycznego jak i do danych w aplikacji po podaniu identyfikatora i właściwego hasła.
3. W przypadku bezczynności użytkownika w pracy na stacji roboczej przez okres dłuższy niż 15 min., automatycznie włączany jest wygaszacz ekranu. Wygaszacz ten powinien być zaopatrzony w hasło analogiczne do hasła systemowego użytkownika.
4. W przypadku, gdy przerwa w pracy na stacji roboczej ma trwać dłużej niż 30 minut użytkownik powinien wylogować się z aplikacji i systemu stacji roboczej na której pracuje.
5. Kończąc pracę użytkownik powinien:
   1) zamknąć programy oraz wylogować się z systemu i wyłączyć komputer wraz z drukarką,
   2) sprawdzić, czy pozostawione stanowisko jest prawidłowo zabezpieczone i czy nie stwarza jakichkolwiek zagrożeń do uruchomienia go przez osoby postronne,
   3) sprawdzić czy w napędach komputera nie pozostały nośniki zawierające dokumenty lub informacje zawierające dane osobowe niejawne lub inne, do których wgląd mogą mieć jedynie wybrani pracownicy Urzędu.
6. Wszystkie zauważone mankamenty w bezpieczeństwie stanowiska, należy bezwzględnie zgłosić ASI.

Rozdział 12

Procedury postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego lub jego składników

§ 21

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń systemu informatycznego, na które mogą wskazywać:
   1) ślady włamania lub prób włamania do obszaru, w którym znajdują się poszczególne elementy systemu np. serwery, stacje robocze lub urządzenia sieciowe,

2) stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),

3) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,

4) błędy w funkcjonowaniu systemu (np. komunikaty informujące o niespójności i błędach w danych, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),

5) znaczne spowolnienie działania systemu informatycznego,

6) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,

7) jest on zobowiązany niezwłocznie powiadomić o tym: bezpośredniego przełożonego, ASI, IOD lub ADO.

2. IOD lub inna upoważniona przez niego osoba powinna w pierwszej kolejności:

1/ zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,

2/ zabezpieczyć miejsce zdarzenia przed ingerencją osób trzecich, aż do jego pełnego wyjaśnienia lub udokumentować jego stan za pomocą np. zdjęć z telefonu komórkowego bądź aparatu czy notatki z opisem,

3/ niezwłocznie podjąć odpowiednie kroki w celu:

1) powstrzymania lub ograniczenia dostępu do systemu i danych osoby niepowołanej,

2) zminimalizowania okoliczności mogących sprzyjać dalszemu powstawaniu szkód ,

3) zabezpieczenie systemu przed usunięciem śladów ingerencji osoby niepowołanej,

4/ na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,

5/ przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do systemu osoby niepowołanej,

6/ przywrócić normalny stan działania systemu.

3. Po wyeliminowaniu bezpośredniego zagrożenia ASI ma obowiązek przeprowadzić analizę stanu systemu informatycznego, a w szczególności sprawdzić:

1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

2) zawartość zbioru danych osobowych,

3) sposób działania programów,

4) jakość komunikacji w sieci telekomunikacyjnej,

5) obecność wirusów komputerowych.

Rozdział 13

Zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych

§ 22

1. Osoba, która zauważyła niepokojące zdarzenie, wystąpienie poniżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania: bezpośredniego przełożonego, ASI, IOD lub ADO.
2. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż ADO, jest ona zobowiązana poinformować o tym fakcie ADO.
3. Naruszeniu ochrony danych osobowych mogą świadczyć symptomy występujące w następujących obszarach:
   1) w obrębie pomieszczeń, szafek lub miejsc przechowywania:
      a) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych , w szczególności do serwerowni oraz kas, gdzie przechowuje są nośniki kopii zapasowych,
      b) włamanie lub próby włamania do szafek, w których przechowywane są , w postaci elektronicznej lub papierowej , nośniki danych osobowych,
   2) w obrębie sprzętu informatycznego:
      a) kradzież komputera, w którym przechowywane są dane osobowe,
      b) rozkręcona obudowa komputera,
   3) w obrębie systemu informatycznego i aplikacji:
      a) brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych,
      b) brak możliwości zalogowania się do tej aplikacji,

c) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji
(na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych),

d) poszerzone uprawnienia w obrębie aplikacji w stosunku do dotychczas przyznanych (na przykład wgląd do szerszego zakresu danych o pracownikach),

e) inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar),

4) Inne

a) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikro-procesorowej, pendrive'a itp.),

b) zagubienie bądź kradzież nośnika z zawartością danych osobowych,

§ 23

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w Urzędzie naruszenia bezpieczeństwa danych osobowych, IOD we współpracy z ASI, jest zobowiązany do podjęcia następujących kroków:

1) stwierdzenia czy rzeczywiście doszło do naruszenia ochrony danych osobowych, w tym:
   a) sprawdzenia okoliczności zdarzenia,
   b) wyjaśnienia jego przyczyn, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,
2) w przypadku, gdy doszło do naruszenia ochrony danych osobowych to:
   a) zebranie ewentualnych dowodów,
   b) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
   c) zabezpieczenia danych przetwarzanych w systemie informatycznym, jego logów systemowych, logów programu i bazy w których nastąpiło naruszenie bezpieczeństwa oraz danych konfiguracyjnych całego systemu w celu późniejszej analizy
   d) usunięcia skutków incydentu i przywrócenia pierwotnego stanu systemu informatycznego
      tj. stanu sprzed incydentu, polegające na:
      - przeprowadzeniu analizy spójności danych osobowych przetwarzanych w systemie,
      - ewentualnym odtworzeniu kopii zapasowych danych i plików konfiguracyjnych,
      - przeprowadzeniu analizy poprawności funkcjonowania systemu informatycznego,
      - powtórnym zabezpieczeniu danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

§ 24

System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

§ 25

IOD określa, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym Urzędu.

§ 26

IOD prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

1) imię i nazwisko osoby zgłaszającej incydent,
2) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
3) datę zgłoszenia incydentu,
4) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
5) wyniki przeprowadzonych działań,
6) podjęte akcje naprawcze i ich skuteczność.

§ 27

IOD odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

1) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
2) określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
3) określenia potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

Rozdział 14

Zasady udostępniania danych osobowych

§ 28

1. Udostępnianie danych osobowych ze zbioru danych, osobom lub podmiotom uprawnionym do ich otrzymania odbywać się może na pisemny, umotywowany wniosek.
2. Decyzję o udostępnieniu danych osobowych podejmuje ADO.
3. Po otrzymaniu zgody od ADO, dane do udostępnienia przygotowuje pracownik Urzędu merytorycznie odpowiedzialny za ich przetwarzanie i integralność w porozumieniu z ASI. ASI jest zobowiązany do odnotowania informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.

Rozdział 15

Wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych.

§ 29

1. Wszelkie dane, a zwłaszcza dane osobowe, które leżą w gestii administrowania i gromadzenia przez Urząd, są przetwarzane w budynku urzędu znajdującym się w Rynie przy ulicy Ratuszowa 2.
2. Szczegółowy wykaz pomieszczeń, w których dane są gromadzone i przetwarzane, ich usytuowanie oraz zabezpieczenie umieszczony jest w „Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Rynie”.
3. W szczególnie uzasadnionych przypadkach możliwe jest przetwarzanie danych osobowych poza

wyznaczonym obszarem (np. na komputerach przenośnych) wyłącznie za zgodą ADO.

Rozdział 16

Zasady dostępu do budynku oraz pomieszczeń, gdzie przetwarzane są dane.

§ 30

1. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe oraz pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają do tego upoważnienie.
2. Kontrolą dostępu do pomieszczeń przeznaczonych do przetwarzania danych osobowych zajmuje się IOD.
3. Przebywanie na terenie Urzędu, po godzinach pracy lub w dni wolne od pracy wymaga ustnej zgody ADO lub poinformowania o tym fakcie ASI w celu zmiany harmonogramu dostępu do systemu informatycznego i monitoringu budynku.

Rozdział 17

Schemat strukturalny wewnętrznej sieci teleinformatycznej z wyszczególnieniem zabezpieczeń, rozmieszczeniem baz danych zawierających dane osobowe oraz komputerów, które je przetwarzają

§ 31

1. Aktualny schemat wewnętrznej struktury sieci teleinformatycznej, rozmieszczenia serwerów, na których zlokalizowane są bazy zawierające dane osobowe oraz opis zabezpieczeń systemowych znajduje się w „Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Rynie".
2. Informacje zamieszczone w Instrukcji powinny być aktualizowane po każdorazowym wprowadzeniu zmian w strukturze sieci bądź jej zabezpieczeniach, wprowadzeniu zmian co do ilości, funkcjonalności czy zabezpieczeń poszczególnych serwerów.

§ 32

1. Aktualny wykaz serwerów i komputerów stanowiskowych, na których znajdują się bazy danych zawierające dane osobowe oraz opis systemów operacyjnych i ich zabezpieczeń przed nieautoryzowanym dostępem zawiera „Instrukcja zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Rynie"
2. Informacje zamieszczone w Instrukcji powinny być aktualizowane po wprowadzeniu zmian co do ilości, funkcjonalności czy zabezpieczeń poszczególnych komputerów/serwerów.

Rozdział 18

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

§ 33

1. Aktualny wykaz zbiorów, w których przetwarzane są dane osobowe wraz ze wskazaniem rodzaju zbieranych danych osobowych i programów zastosowanych do ich przetwarzania, podaje się do publicznej wiadomości.
2. Informacje zamieszczone w wykazie zbiorów powinny być aktualizowane po wprowadzeniu zmian co do ilości lub funkcjonalności zbiorów danych osobowych oraz po zmianie oprogramowania służącego do ich przetwarzania.

Rozdział 19

Opis struktur zbiorów danych

§ 34

1. Aktualny opis struktur zbiorów danych i powiązania między nimi znajduje się w „Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Rynie" .
2. Informacje zamieszczone w Instrukcji powinny być aktualizowane po wprowadzeniu istotnych zmian w strukturach baz danych, które opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany rejestruje się bezpośrednio aktualizując przedmiotowy dokument, nie rzadziej niż co 2 miesiące.

Rozdział 20

sposób przepływu danych pomiędzy poszczególnymi systemami

§ 35

1. Aktualny opis sposobu przepływu danych pomiędzy poszczególnymi systemami znajduje się w „Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy w Rynie"
2. Informacje zamieszczone w Instrukcji powinny być aktualizowane po wprowadzeniu istotnych zmian w strukturach baz danych i związanych z tym zmian w zakresie bądź sposobie wymiany informacji pomiędzy nimi. W przypadku systemów, które są rozbudowywane wprowadzone zmiany rejestruje się (aktualizując dokument) nie rzadziej niż co 2 miesiące.

Rozdział 21

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

§ 36

Zasady ogólne

1. Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje stu procentowego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik mający styczność

z przetwarzanymi danymi, świadom odpowiedzialności, postępował zgodnie z przyjętymi w niniejszym dokumencie zasadami i minimalizował zagrożenie wynikające z błędów ludzkich.

2. Ochrona danych osobowych przetwarzanych w Urzędzie obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w Urzędzie, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.
3. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
4. Przetwarzać dane osobowe w systemach informatycznych jak i tradycyjnych zbiorach papierowych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych otrzymane od ADO.
5. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
6. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
7. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
8. Zachowanie tajemnicy służbowej obowiązuje pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
9. IOD i ADO jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie Urzędu.

§ 37

Środki organizacyjne

1. Wprowadzenie Polityki bezpieczeństwa w zakresie przetwarzania i ochrony danych osobowych oraz Instrukcji zarządzania systemem informatycznym .
2. Wyznaczenie IOD i ASI odpowiedzialnych za działania organizacyjne i środki techniczne zapewniające odpowiedni poziom bezpieczeństwa danych osobowych.
3. Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz rejestrowanie czynności przetwarzania danych..
4. Kontrola dostępu do pomieszczeń, w których przetwarzane są dane osobowe oraz ścisła kontrola dostępu do pomieszczeń, w których znajdują się serwery.

§ 38

Środki techniczne

1. Zabezpieczenia fizyczne:
   1) W siedzibie Urzędu jest monitoring pod nadzorem służb ochrony zewnętrznej.
   2) Poszczególne pomieszczenia, w których odbywa się przetwarzanie danych i ich składowanie wyposażono w drzwi z niezależnymi zamkami, które są zamykane podczas nieobecności pracowników. Po zakończeniu pracy osoba zamykająca pomieszczenie powinna dodatkowo sprawdzić czy zostały w nim zamknięte wszystkie okna i wyłączone wszystkie komputery;
2. Pozostałe formy zabezpieczeń:
   1) Stanowiska komputerowe w pomieszczeniach, gdzie mogą czasowo przebywać osoby

nieupoważnione do przetwarzania danych osobowych, powinny być tak usytuowane, aby uniemożliwić takim osobom wgląd w przetwarzane dane zarówno na monitorach jak i wydrukach;
2) Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym;
3) Zbędne lub nieaktualne wydruki powinny być bezwzględnie niszczone w niszczarkach.

Środki informatyczne

1) Ustalenie i przestrzeganie polityki dostępu do komputerów i programów przetwarzających dane za pomocą identyfikatorów i haseł;
2) Zgodne z „Instrukcją zarządzania systemem informatycznym" tworzenie kopii baz danych zawierających dane osobowe;
3) Bardzo dokładne testowanie modyfikacji oprogramowania przed wdrożeniem go do użytku produkcyjnego zarówno pod kątem poprawności działania jak i podatności na „ataki" z zewnątrz;
4) Ustalenie polityki ochrony antywirusowej, skanowania sieci i stanowisk komputerowych oraz przestrzeganie ustalonego harmonogramu;
5) Ustalenie polityki aktualizacji systemów operacyjnych pracujących na wszystkich komputerach Urzędu;
6) Utworzenie harmonogramu sprawdzania aktualizacji systemów i programów na stacjach roboczych;
7) W przypadku dłuższej bezczynności w pracy stanowiska komputerowego, automatycznie powinien uruchomić się wygaszacz ekranu chroniony hasłem lub użytkownik powinien sam zablokować stację tak, aby jej ponowne użycie było możliwe po podaniu hasła dostępu;

Rozdział 22

Sposób postępowania w zakresie komunikacji poza siecią lokalną

§ 39

Przy przesyłaniu danych osobowych poza siecią dedykowaną do transferu danych osobowych wymagane jest zastosowanie szczególnych wymagań w zakresie bezpieczeństwa. Obejmują one:

1) Zatwierdzenia w formie pisemnej lub w formie elektronicznej przez ADO celu wysłania danych osobowych,
2) Zastosowanie mechanizmów szyfrowania danych osobowych,

§ 40

W przypadku stosowania mechanizmów kryptograficznych ADO określa wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych. Jeżeli nie określi on innych wymagań stosuje się:

1) przy szyfrowaniu symetrycznym algorytm AES z kluczem 256 bitów,
2) przy szyfrowaniu asymetrycznym algorytm RSA z kluczem 1024 bity,
3) funkcję skrótu SHA-1.

§ 41

W wypadku, gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe, korzysta z innych mechanizmów kryptograficznych niż stosowane w Urzędzie, możliwe jest zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych. W tym celu ASI lub osoba specjalnie do tego celu wyznaczona, może przeprowadzić analizę poziomu bezpieczeństwa mechanizmu kryptograficznego oraz zgodności tego mechanizmu z komponentami systemu informatycznego.

§ 42

W przypadku wystąpienia uzasadnionego podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce pracownik zobowiązany jest poinformować o tym fakcie osoby uprawnione.

Rozdział 23

Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe poza siedzibą urzędu

§ 43

Przetwarzanie danych osobowych na komputerach przenośnych poza siedzibą Urzędu, powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie na podstawie pisemnej zgody ADO. Zakres, czas oraz miejsce przetwarzania powinno być ustalone przez przełożonego pracownika i uzgodnione z IOD oraz ASI.

§ 44

Pracownik korzystający z komputera przenośnego do przetwarzania danych osobowych lub dokumentów stanowiących tajemnicę służbową, zwłaszcza mających charakter lokalnej bazy lub pliku czyli zlokalizowanych bezpośrednio na użytkowanym komputerze i przetwarzanie których odbywa się poza obszarem, o którym mowa w rozdziale 5 „Instrukcji zarządzania systemem informatycznym", zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. W związku z powyższym użytkownik komputera przenośnego zobowiązanyjest do:

1) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 –mio znakowym zawierającym : duże i małe litery, znaki specjalne lub cyfry,
2) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
   a) transportowania komputera w odpowiedniej, przeznaczonej do tego celu torbie jako bagażu poręcznego,
   b) nie pozostawiania komputera w samochodzie, przechowalni bagażu, środkach transportu publicznego itp,
3) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
4) zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym),
5) zabezpieczenia komputera przenośnego hasłem i utrzymanie konfiguracji oprogramowania

systemowego w stanie wymuszającym korzystanie z tego hasła,
6) wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
7) zmianę haseł zgodnie z harmonogramem przyjętym w Urzędzie,
8) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,
9) regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego Urzędu w celu umożliwienia wykonania kopii awaryjnej,
10) cyklicznego podłączania komputera do sieci informatycznej Urzędu w celu wykonania aktualizacji wzorców wirusów w programie antywirusowym,

§ 45

ASI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności:
1) dokonać konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł odpowiedniej jakości oraz ich cyklicznej zmiany, zgodnie z wytycznymi dotyczącymi polityki posługiwania się hasłami w systemie informatycznym Urzędu,
2) w przypadku przetwarzania danych osobowych znajdujących się bezpośrednio na komputerze przenośnym - zabezpieczyć je dodatkowo poprzez wykorzystanie oprogramowania szyfrującego
3) dokonać instalacji i konfiguracji oprogramowania antywirusowego,
4) przeprowadzić aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

§ 46

ASI jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych poza siedzibą Urzędu. W szczególności ewidencja powinna obejmować:
1) typ i numer seryjny komputera przenośnego,
2) imię i nazwisko osoby będącej użytkownikiem komputera,
3) wykaz oprogramowania zainstalowanego na komputerze, służącego do przetwarzania danych osobowych
4) rodzaj i zakres danych osobowych przetwarzanych na komputerze.

§ 49

W razie zgubienia lub kradzieży komputera przenośnego, pracownik zobowiązany jest do natychmiastowego powiadomienia IOD lub osoby uprawnionej zgodnie z zasadami informowania w przypadku naruszenia ochrony danych osobowych.

Rozdział 24

Przetwarzanie danych powierzonych Urzędowi przez inne podmioty

§ 50

Możliwe jest przetwarzanie w Urzędzie danych osobowych powierzonych przez inny podmiot

(Zleceniodawcę). W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie porozumienia pomiędzy Urzędem a Zleceniodawcą zawartego w formie pisemnej.
Porozumienie to musi zawierać ściśle określony zakres przetwarzanych danych.
Powierzone dane podlegają ochronie na takich samych zasadach jak dane będące własnością Urzędu, chyba, że porozumienie określi inne zasady ich ochrony, w szczególności może dotyczyć to nadawania uprawnień do przetwarzania danych osobowych.

Rozdział 25

Postanowienia końcowe

§ 51

Wszyscy pracownicy są zobowiązani do zapoznania się z treścią niniejszej polityki.

§ 52

Polityka bezpieczeństwa wchodzi w życie z dniem podpisania.

§ 53

Jakiekolwiek zmiany wprowadzane w załącznikach do niniejszego dokumentu nie wymagają zmiany zarządzenia, które wprowadziło niniejszą instrukcję w życie.

Załącznik Nr 2
do Zarządzenia Nr 62
Burmistrza Miasta i Gminy Ryn
z dnia 24.05.2018r.

„Instrukcja
zarządzania systemem informatycznym
w Urzędzie Miasta i Gminy Ryn”

§ 1.

Zarządzanie systemami haseł.

1. Osobą odpowiedzialną za sposób przydziału haseł użytkownikom oraz częstotliwość ich zmiany jest osoba zatrudniona jako informatyk w Urzędzie Miasta i Gminy Ryn .
2. Każdy użytkownik systemu informacyjnego ma przydzielony jednorazowo niepowtarzalny identyfikator oraz okresowo zmieniane hasło dostępu.
3. Dostęp do zasobów systemów odbywać się może tylko w oparciu o system haseł przydzielanych indywidualnie pracownikom oraz użytkownikom systemu.
4. Zapewnione jest generowanie haseł w cyklu miesięcznym. Użytkownicy mają obowiązek zmieniać swoje hasło nie rzadziej niż co 30 dni.
5. Użytkownik nie może udostępniać swego hasła innym osobom.
6. Przekazywanie haseł odbywa się w sposób poufny i nie może ono być zapisywane w miejscu pozwalającym na dostęp dla osób nieupoważnionych.
7. W przypadku utraty hasła lub istnienia podejrzenia naruszenia systemu haseł przez osoby nieuprawnione, dotychczasowy zestaw haseł musi być niezwłocznie unieważniony i zastąpiony nowym.

§ 2.

Zasady rejestrowania i wyrejestrowywania użytkowników.

1. Osobą odpowiedzialną za rejestrowanie i wyrejestrowywanie użytkowników w jednostce jest osoba zatrudniona jako informatyk w Urzędzie Miasta i Gminy Ryn.
2. Podstawą do zarejestrowania użytkownika do danego systemu przetwarzania danych jest zakres czynności pracownika, w którym musi być jawnie wskazane, że dana osoba ma za zadanie pracować przy przetwarzaniu danych danego systemu w podanym zakresie. Natomiast podstawą do wyrejestrowania użytkownika z danego systemu przetwarzania danych jest nowy zakres czynności pracownika lub jego zwolnienie.
3. Administrator rejestruje oraz wyrejestrowuje użytkowników, prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych archiwizując identyfikator, imię i nazwisko użytkownika. Wykaz użytkowanego oprogramowania i jego użytkowników stanowi załącznik nr 1.
4. Identyfikatory osób, które utraciły uprawnienia dostępu do danych, należy wyrejestrować z systemu, unieważniając przekazane hasła. Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.
5. Osoby dopuszczone do przetwarzania danych zobowiązane są do zachowania tajemnicy (dostępu do danych i ich merytorycznej treści). Obowiązek ten istnieje również po ustaniu zatrudnienia.

§ 3.

Procedury rozpoczęcia i zakończenia pracy.

1. Użytkownicy przed przystąpieniem do pracy przy przetwarzaniu danych powinni zwrócić uwagę, czy nie istnieją przesłanki do tego, że dane zostały naruszone. Jeżeli istnieje takie podejrzenie, należy postępować zgodnie z „Instrukcją postępowania w sytuacji naruszenia zasad ochrony systemów informatycznych".
2. Dostęp do konkretnych zasobów danych jest możliwy dopiero po podaniu właściwego identyfikatora i hasła dostępu.
3. Hasło użytkownika należy podawać do systemu w sposób dyskretny (nie literować, nie czytać na głos, wpisywać osobiście, nie pozwalać na bezpośrednią obecność drugiej osoby podczas wpisywania hasła, itp.).
4. Użytkownik ma obowiązek zamykania systemu, programu komputerowego po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem, programem nie może pozostawać bez kontroli pracującego na nim użytkownika.
5. Pomieszczenia, w których znajdują się urządzenia służące do przetwarzania danych oraz wydruki lub inne nośniki zawierające dane, pod nieobecność personelu muszą być zamknięte.

§ 4.

Obsługa kopii bezpieczeństwa, nośników informacji oraz wydruków.

1. Wydruki z systemów informatycznych oraz inne nośniki informacji muszą być zabezpieczone w sposób uniemożliwiający do nich dostęp przez osoby nieupoważnione w każdym momencie przetwarzania, a po upływie czasu ich przydatności są niszczone lub archiwizowane w zależności od kategorii archiwalnej.
2. Wydruki, maszynowe nośniki informacji (dyskietki, dyski optyczne, inne nośniki pamięci masowych, itp.) oraz inne dokumenty, zawierające dane przeznaczone do likwidacji, muszą być pozbawione zapisów lub w przypadku gdy jest to możliwe, muszą być trwale uszkodzone w sposób uniemożliwiający odczytanie z nich informacji.
3. Urządzenia, dyski i inne informatyczne nośniki danych zawierające dane przed ich przekazaniem innemu podmiotowi, winny być pozbawione zawartości. Naprawa wymienionych urządzeń zawierających dane, jeżeli nie można danych usunąć, winna być wykonywana pod nadzorem osoby upoważnionej. W przypadku potrzeby odzyskania danych obowiązkowo należy podpisać z podmiotem, któremu powierza się sprzęt.

§ 5.

Ochrona danych przed ich utratą z systemów informatycznych.

1. Urządzenia i systemy informatyczne zasilane energią elektryczną powinny być zabezpieczone przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (zasilacze awaryjne UPS).

2. Włamanie do pomieszczeń, w których przetwarza się dane powinno być uniemożliwione poprzez zabezpieczenie okien i drzwi wejściowych.
3. Pomieszczenia komputerowe powinny być zabezpieczone przed pożarem.
4. Instalacja oprogramowania może odbywać się tylko przez administratora lub pod jego nadzorem.
5. W celu ochrony przed wirusami komputerowymi, używanie nośników danych (np. dyskietki, dyski optyczne, itp.) spoza jednostki jest dopuszczalne dopiero po uprzednim sprawdzeniu ich przez administratora i upewnieniu się, że nośniki te nie są „zarażone" wirusem.
6. W przypadku stwierdzenia obecności wirusów komputerowych w systemie należy postępować zgodnie z „Instrukcją postępowania w sytuacji naruszenia zasad ochrony systemów informatycznych".

§ 6.

Sposób komunikacji w zakresie sieci komputerowej.

Przesyłanie danych na nośnikach zewnętrznych (np. płyty, nośniki pamięci, wydruki) na zewnątrz jednostki może odbywać się tylko w formie przesyłki poleconej.

§ 7.

Przeglądy i konserwacja systemów i zbiorów danych.

1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje administrator systemu informacji (ASI) co najmniej raz w miesiącu.

2. Ocenie podlegają stan techniczny urządzeń (komputery, serwery, UPS-y, itp.), stan okablowania budynku w sieć logiczną, spójność baz danych, stan zabezpieczeń fizycznych (zamki, kraty), stan rejestrów systemów serwera lokalnej sieci komputerowej.

§ 8.

Postępowanie w sytuacjach naruszenia zasad ochrony systemów informatycznych.

1. Możliwe sytuacje świadczące o naruszeniu zasad ochrony danych przetwarzanych w systemie informatycznym.
Każde domniemanie, przesłanka, fakt wskazujący na naruszenie zasad ochrony danych, a zwłaszcza stan różny od ustalonego w systemie informatycznym, w tym:
1) stan urządzeń (np. brak zasilania, problemy z uruchomieniem),
2) stan systemu zabezpieczeń obiektu,
3) stan aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,
4) zawartość zbioru danych (np. brak lub nadmiar danych),
5) ujawnione metody pracy,

6) sposób działania programu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),
7) przebywanie osób nieuprawnionych w obszarze przetwarzania danych,
8) inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego (np. obecność wirusów komputerowych) – stanowi dla osoby uprawnionej do przetwarzania danych, podstawę do natychmiastowego działania.

2. Sposób postępowania.
1) O każdej sytuacji odbiegającej od normy, a w szczególności o przesłankach naruszenia zasad ochrony danych w systemie informatycznym, opisanych w pkt. 1, należy:
– natychmiast informować administratora lub osobę przez niego upoważnioną,
– niezwłocznie taką sytuację zarejestrować w dzienniku administratora.
2) Osoba stwierdzająca naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo, zobowiązana jest do możliwie pełnego udokumentowania zdarzenia, celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.
3) Stwierdzone przez administratora naruszenie zasad ochrony danych osobowych wymaga powiadomienia kierownika jednostki oraz natychmiastowej reakcji poprzez:
– usunięcie uchybień (np. wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów komputerowych z systemu, itp.),
– zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,
– wstrzymanie przetwarzania danych do czasu usunięcia awarii systemu informatycznego.

Załącznik Nr 1 do „Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Ryn”

Wykaz użytkowanego oprogramowania i jego użytkowników.

Lp.	Zbiór danych	Stanowisko Pracy	Program	Lokalizacja bazy danych	Miejsce przetwarzania danych
1. 2. 3.	Dane podatników. Dane podatków od środków transportowych. Dane windykacji podatkowej.	Stan. pracy ds. podatków i opłat	PUMA - ZetoSoftware, :Podatki, :Pojazdy – podatek od środków transportowych :Windykacja	Serwer UMiG Ryn	Stan. pracy ds. podatków i opłat
4. 5.	Dane związane z finansami jednostki samorządu, prowadzenie ksiąg finansowych budżetu urzędu, podległych jednostek budżetowych.	Stan. pracy ds. księgowości budżetowej, Skarbnik Gminy	PUMA - ZetoSoftware, moduł :Finansowe i Księgowość, :Budżet	Serwer UMiG Ryn	Stan. pracy ds. księgowości budżetowej, Skarbnik Gminy
6. 7.	Dane osobowe kadr i płac. Dane związane z obsługą dodatków mieszkaniowych i energetycznych.	Stan. pracy ds. gospodarki komunalnej i mieszkaniowej	PUMA - ZetoSoftware, moduł Kadry, Płace	Serwer UMiG Ryn	Stan. pracy ds. gospodarki komunalnej i mieszkaniowej
8. 9. 10. 11. 12.	System ewidencji ludności. System obsługi wyborców. System obsługi statystyk ewidencji. Informacje o nr PESEL i zameldowaniu. System wydawania dowodów osobistych.	Urząd Stanu Cywilnego	PUMA - ZetoSoftware, :Ewidencja Ludności, :Wyborcy, :Statystyki	Serwer UMiG Ryn System Rejestrów Państwowych	Urząd Stanu Cywilnego
13.	Dane użytkowników programu,	Informatyk	PUMA - ZetoSoftware, moduł administracyjn	Serwer UMiG Ryn	Informatyk

Lp.	Zbiór danych	Stanowisko Pracy	Program	Lokalizacja bazy danych	Miejsce przetwarzania danych
			y i techniczny dostęp do wszystkich modułów		
14.	Wspólny moduł danych osobowych i adresowych kontrahentów.	Wszyscy użytkownicy programu PUMA.	PUMA - ZetoSoftware, moduł Kontrahenci	Serwer UMiG Ryn	Wszyscy użytkownicy programu PUMA.
15.	System ewidencji gruntów i budynków oraz ich wizualizacja.		Geobid - Ewopis,		Stan. pracy ds. gospodarki gruntami i obrotu nieruchomościami,
16. 17.	Dane osób rejestrujących działalność gospodarczą Dane wnioskodawców o stypendia		Centralna Ewidencja i Informacja o Działalności Gospodarczej Sygnity - Świadczenia Rodzinne, Stypendia	Rejestr Państwowy CEIDG Serwer UMiG Ryn	Stan. pracy ds. działalności gospodarczej, oświaty, kultury, sportu i turystyki
18.	Dane dokumentów ubezpieczeniowych.	Stan. pracy ds. księgowości budżetowej	Płatnik - obsługa dokumentów ZUS, Asseco Poland SA.	Stan. pracy ds. księgowości budżetowej	Stan. pracy ds. księgowości budżetowej
19.	Elektroniczna platforma obsługi wyborów	Urząd Stanu Cywilnego, Informatyk, Sekretarz Gminy	Platforma Wyborcza WOW	System Państwowy	Urząd Stanu Cywilnego, Informatyk, Sekretarz Gminy
20.	Elektroniczna obsługa przelewów bankowych	Stan. pracy ds. księgowości budżetowej	Bankowość elektroniczna	Mazurski Bank Spółdzielczy	Stan. pracy ds. księgowości budżetowej
21.	Dane adresowe w odpowiedziach do petentów i wykazach	Wszystkie stanowiska urzędnicze UMiG Ryn	Pakiet biurowy MS Office/ Libreoffice	Wszystkie stanowiska urzędnicze UMiG Ryn	Wszystkie stanowiska urzędnicze UMiG Ryn