BURMISTRZ DRAWNA
73-220 DRAWNO
ul. Kościelna 3
woj. zachodniopomorskie
tel. (95) 768-20-31

ZARZĄDZENIE Nr 36 / 2016
Burmistrza Drawna
z dnia 27 czerwca 2016r.

w sprawie ochrony danych osobowych w Urzędzie Miejskim w Drawnie oraz powierzenia obowiązków w zakresie ochrony danych osobowych

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (t. j. Dz. U. z 2016r. poz. 446) oraz art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182 ze zm.) w związku z § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100 poz. 1024) zarządzam, co następuje:

§ 1. W celu ustalenia zasad postępowania w procesach przetwarzania danych osobowych oraz ochrony interesów osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych w Urzędzie Miejskim w Drawnie, wprowadzam jako obowiązującą dokumentację bezpieczeństwa informacji.
2. Każda osoba mająca dostęp do danych osobowych przetwarzanych w Urzędzie jest zobowiązana do zapoznania się z dokumentacją, o której mowa w § 2.

§ 2. Dokumentację, o której mowa w § 1 ust. 1 stanowią:
1) „Polityka bezpieczeństwa informacji" – stanowiąca załącznik nr 1 do niniejszego Zarządzenia,
2) „Instrukcja zarządzania systemem informatycznym w Urzędzie Miejskim w Drawnie" – stanowiąca załącznik nr 2 do niniejszego Zarządzenia,
3) „Regulamin określający zasady i procedury korzystania z e sprzętu komputerowego, oprogramowania, sieci teleinformatycznej oraz poczty elektronicznej Urzędu" – stanowiący załącznik nr 3 do niniejszego Zarządzenia.

§ 3. 1. Powierzam kierownikowi referatu organizacyjno-administracyjnego obowiązki koordynatora ds. ochrony danych osobowych w Urzędzie Miejskim w Drawnie.
2. Powierzam Panu Filipowi Sońta obowiązki Administratora systemu informatycznego w Urzędzie Miejskim w Drawnie.

§ 4. Szczegółowy zakres obowiązków Koordynatora ds. ochrony danych osobowych oraz Administratora systemu informatycznego został określony w Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Drawnie oraz w Instrukcji zarządzania systemem informatycznym w Urzędzie Miejskim w Drawnie.

§ 5. Zobowiązuję wszystkie osoby dopuszczone do przetwarzania danych osobowych do współpracy z Koordynatorem ds. ochrony danych osobowych oraz Administratorem systemu informatycznego w zakresie określonym w Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Drawnie oraz w Instrukcji zarządzania systemem informatycznym w Urzędzie Miejskim w Drawnie.

§ 6. Traci moc Zarządzenie Nr 33/05 Burmistrza Drawna z dnia 12 grudnia 2005r. w sprawie ochrony danych osobowych oraz użytkowników systemów informatycznych.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ DRAWNA

mgr inż. Andrzej Okmielewski

Załącznik Nr 1
do Zarządzenia Nr 36/2016
Burmistrza Drawna z dnia 27 czerwca 2016r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W DRAWNIE

POSTANOWIENIA OGÓLNE

§ 1. Polityka bezpieczeństwa została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 ze zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100 poz. 1024).

§ 2. 1. Polityka bezpieczeństwa określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
2. Polityka bezpieczeństwa służy zapewnieniu wysokiego bezpieczeństwa przetwarzanych danych osobowych.
3. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 3. Ilekroć w Polityce bezpieczeństwa jest mowa o:

1) Urzędzie – rozumie się przez to Urząd Miejski w Drawnie,
2) Polityce – rozumie się przez to politykę Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Drawnie'
3) zbiorze danych osobowych – rozumie się przez to każdy posiadający strukturę danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
5) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
6) systemie tradycyjnym – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze,
7) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
8) zabezpieczaniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
9) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

10) Administratorze danych osobowych (ADO) - rozumie się przez to kierownika jednostki, który decyduje o celach i środkach przetwarzania danych osobowych,
11) koordynatorze – rozumie się przez to osobę upoważnioną przez Burmistrza Drawna do koordynowania realizacji zadań wynikających z ustawy o ochronie danych osobowych,
12) Administratorze Systemu Informatycznego (ASI) – rozumie się przez to osobę upoważnioną przez Burmistrza Drawna do realizacji zadań związanych z zarządzaniem systemem informatycznym,
13) użytkowniku systemu informatycznego - rozumie się przez to pracownika upoważnionego przez Burmistrza Drawna wyznaczonego do przetwarzania danych osobowych.

Rozdział I
CELE

§ 4. Dane osobowe w Urzędzie Miejskim w Drawnie są gromadzone, przechowywane, edytowane i archiwizowane na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 5. Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się w swojej treści do informacji:

1) w formie papierowej – przetwarzanej w ramach systemu tradycyjnego,
2) w formie elektronicznej – przetwarzanej w ramach systemu informatycznego.

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

§ 7. Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Urzędu Miejskiego w Drawnie oraz innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie.

§ 8. 1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i która wyraziła zgodę na ich przetwarzanie.
2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.
3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.
4. Ocena niezbędności przetwarzania danych do wypełniania usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji.

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

1) adresie swojej siedziby i pełnej nazwie,

2) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Przepisu ust. 1 nie stosuje się jeżeli:

1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

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

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

1) adresie swojej siedziby i pełnej nazwie,
2) celu i zakresie zbieranych danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3) źródle danych,
4) prawie dostępu do treści swoich danych oraz ich poprawiania,
5) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełniania usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza prawa i wolności osoby, której dane dotyczą,
6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełniania usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Przepisu ust. 1 nie stosuje się , jeżeli:

1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
2) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badań,
3) dane są przetwarzane przez Administratora danych na podstawie przepisów prawa,
4) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

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

§. 11. Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują kierownicy referatów Urzędu.

§ 12. 1. Z zasadami Polityki bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik **Nr 1** do niniejszej Polityki bezpieczeństwa.
2. Oświadczenie przechowywane jest w aktach osobowych pracownika a drugi egzemplarz w dokumentacji Administratora danych.

§ 13. 1. Do danych osobowych przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy urzędu Miejskiego w Drawnie oraz osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik **Nr 2** do niniejszej Polityki bezpieczeństwa. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy.
2. Upoważnienie określone w ust. 1 przechowywane jest w aktach osobowych pracownika a drugi egzemplarz w dokumentacji Administratora danych.
3. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi koordynator.
4 Wzór ewidencji określonej w ust. 3 stanowi załącznik **Nr 3** do niniejszej Polityki bezpieczeństwa.

§ 14. 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 odpowiednimi środkami technicznymi.

Rozdział II
ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 15. 1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator danych.
2. Kierownicy referatów obowiązani są zastosować w swoich referatach środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszaniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 16. Administrator danych wyznacza koordynatora ochrony danych osobowych w Urzędzie. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochroną przetwarzanych danych osobowych.

§ 17. 1. Koordynator wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.
2. Koordynator jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak aby wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.
3. Koordynator posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.
4. Szczegółowy zakres odpowiedzialności i obowiązków koordynatora ochrony danych osobowych jest następujący:

1) zapewnienie przestrzegania przepisów o ochronie danych osobowych przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   b) nadzorowanie opracowania i aktualizacji dokumentacji , o której mowa w art. 36 ust. 1 i 2, oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (szkolenia),
2) prowadzenie rejestru zbiorów danych przetwarzanych przez Administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7,
3) nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych,
4) nadzoruje przestrzeganie przez wszystkich użytkowników stosowania obowiązujących procedur,
5) weryfikuje listę autoryzowanych użytkowników systemów informatycznych,
6) dba, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa,
7) prowadzi kontrolę w zakresie bezpieczeństwa systemów,
8) prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych,
9) przygotowuje wnioski pokontrolne dla Administratora danych.

§ 18. 1. Administrator danych wyznacza Administratora Systemu Informatycznego (ASI), który posiada wyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.
2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.
3. Szczegółowy zakres odpowiedzialności i obowiązków ASI jest następujący:
   1) monitoruje oraz zapewnia ciągłość działania systemu informatycznego,
   2) realizuje decyzje Administratora danych odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narządzi służących do ich przetwarzania, w środowisku IT Urzędu tj.:
   a) tworzenie kont użytkowników w systemach informatycznych,

b) przypisywanie, do kont, startowych haseł uwierzytelniających użytkowników tych kont,
c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
d) resetowanie utraconych haseł,
e) usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie,
f) dostarczanie Administratorowi danych potrzebnych do oceny prawidłowości funkcjonowania sprzętu i oprogramowania,
3) odpowiada za bezpieczeństwo systemu informatycznego,
4) zobowiązuje i na bieżąco kontroluje stosowanie się użytkowników systemu do obowiązujących procedur,
5) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego,
6) zapewnia aktualizację dokumentacji technicznej systemu informatycznego w tym opis struktur zbiorów i ich zależności,
7) planuje i wykonuje zadania związane z tworzeniem kopii bezpieczeństwa systemów i danych,
8) monitoruje legalności oprogramowania wykorzystywanego na stacjach roboczych,
9) zapewnia serwerom i stacjom roboczym niezbędnych licencji programowych,
10) systematycznie aktualizuje oprogramowanie systemowe, aplikacyjne i ochronne,
11) zapewnia eksploatowanym systemom opiekę serwisoweą producenta – zawieranie umów regulujących formy tej opieki,
12) rozwiązuje samodzielnie i we współpracy z pozostałymi użytkownikami systemu problemy towarzyszące eksploatacji systemów informatycznych,
13) przygotowuje, we współpracy z koordynatorem, instrukcje dla użytkowników systemów informatycznych zgodne z celami i metodologią wdrożonej polityki bezpieczeństwa informacji,
14) prowadzi szkolenia na temat bezpiecznych zachowań użytkowników w środowisku systemów IT.

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

1)kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników,
2)kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie,
3)zgłasza koordynatorowi planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie,
4)wnioskuje o nadanie upoważnień do przetwarzania danych osobowych podległym pracownikom,
5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Urzędzie.

§ 20. Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy, również z wykorzystaniem stacji roboczej. Jest

odpowiedzialny przed Administratorem danych za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

Rozdział III
WYKAZA BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

§ 21. 1. Miejscem przetwarzania danych osobowych jest budynek Urzędu Miejskiego w Drawnie przy ul. Kościelnej 3 i budynek Spichlerza przy ul. Jeziornej 2.
2. Dane osobowe są przetwarzane w pomieszczeniach lub częściach pomieszczeń budynku.
3. Wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi załącznik **nr 4** do niniejszej polityki.

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

§ 22. 1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych referatów Urzędu w postaci dokumentów papierowych i w systemie informatycznym.
2. Wykaz zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik **Nr 5** do niniejszej polityki.

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

1) dane osobowe zwykłe – wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych,
2) dane osobowe szczególnie chronione – zgodnie z art. 27 ust. 1 ustawy o ochronie danych osobowych wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

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

Rozdział V
STRUKTURY ZBIORÓW DANYCH OSOBOWYCH , POWIĄZANIA MIĘDZY NIMI ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 25. 1. Opis struktury danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa załącznik **nr 6** do niniejszej Polityki.
2. Opis struktury zbiorów prowadzony jest przez Administratora Systemu Informatycznego.
3. Przekazywanie danych (informacji) w systemie informatycznym poza sieć lokalną Urzędu odbywa się w relacji Urząd – mieszkańcy, przedsiębiorcy, kontrahenci, ZUS, US, Benki, NFOZ, Urząd Wojewódzki, Urząd Marszałkowski oraz inne jednostki administracji samorządowej i rządowej.

Rozdział VI
OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 26. Ze względu na to, że dane osobowe przetwarzane są również w systemie informatycznym, który połączony jest z siecią publiczną należy zapewnić wysoki poziom bezpieczeństwa.

1. **Środki ochrony fizycznej:**

1) Budynek Urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych zamykany jest po zakończeniu pracy i zabezpieczony roletami antywłamaniowymi,
2) urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi,
3) w pomieszczeniu serwerów zainstalowano metalowe drzwi zamykane na zamek patentowy,
4) przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności kierownika referatu,
5) pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich,
6) w przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane,
7) do przebywania w pomieszczeniu serwera uprawnieni są : Administrator danych, Administrator Systemu Informatycznego i koordynator ochrony danych osobowych,
8) przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o

których mowa w pkt. 7, a w przypadku ich nieobecności – w obecności osoby pisemnie upoważnionej przez Burmistrz Drawna.

2. Środki sprzętowe, informatyczne i telekomunikacyjne:

1) każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki dokumentów),
2) urządzenia wchodzące w skład systemu informatycznego podłączone są do obwodu elektrycznego, zabezpieczonego na wypadek zanikania napięcia albo awarii w sieci zasilającej centralnym UPS-em,
3) sieć lokalna podłączona do Internetu za pomocą odrębnego komputera spełniającego funkcje Firewall'a (zapora ogniowa),
4) zastosowano oprogramowanie do tworzenia kopii zapasowych,
5) wszystkie serwery i stacje robocze muszą posiadać zainstalowany program antywirusowy. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do użytkownika,
6) archiwizacje wykonywane są na płytach CD oraz na odrębnym komputerze zabezpieczonym hasłem w zamykanym pomieszczeniu.

3. Środki ochrony w ramach oprogramowania systemu:

1) dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługą informatyczną Urzędu,
2) konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji,
3) system informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1) zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji,
2) dla każdego użytkownika systemu jest ustalony odrębny identyfikator,
3) zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

5. Środki ochrony w ramach systemu użytkowego:

1) zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika,
2) komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

6. Środki organizacyjne:

1) Administrator Danych Osobowych przyznaje uprawnienia w zakresie dostępu do systemu informatycznego określającego zakres uprawnień pracownika,
2) osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem ich do pracy z tymi danymi są szkolone w zakresie obowiązujących przepisów o ochronie

danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.

3) każdy pracownik podpisze oświadczenie stanowiące załącznik Nr 1,
4) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
5) wprowadzono instrukcję zarządzania systemem informatycznym,
6) określono procedury postępowania w sytuacji naruszenia ochrony danych osobowych,
7) powinno się dążyć, aby nośniki były opisane i ewidencjonowane,
8) wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu informatycznego, działań konserwacyjnych w systemie oraz naprawy systemu,
9) określono sposób postępowania z nośnikami informacji,
10) wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy dopiero po uzyskaniu zgody Administratora danych.

Rozdział VII
UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

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

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

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

Rozdział VIII
POSTĘPOWANIE W PRZYPADKU NARUSZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

§ 28. 1. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić koordynatora o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie.
2. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:

1) stanu urządzeń technicznych,
2) zawartości zbioru danych osobowych,
3) sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej,
4) metod pracy (w tym obiegu dokumentów),

5) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.).

3. W przypadku stwierdzenia naruszenie ochrony danych osobowych należy niezwłocznie:

1) powiadomić koordynatora lub bezpośredniego przełożonego,
2) zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych,
3) niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony (o ile to możliwe),
4) zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu,
5) zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia.

4. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych koordynator podejmuje czynności wyjaśniające mające na celu ustalenie:

1) przyczyn i okoliczności naruszenia ochrony,
2) zapoznania się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy urzędu,
3) osób winnych naruszenia danych osobowych,
4) skutków naruszenia, w tym rozważa celowość kontaktu ze specjalistami spoza Urzędu (jeśli zachodzi taka potrzeba).

5. Koordynator zobowiązany jest powiadomić Administratora danych, który podejmuje czynności zmierzające do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.
6. Koordynator zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, który stanowi załącznik **Nr 7** do niniejszej Polityki.
7. Raport z wystąpienia zdarzenia koordynator przekazuje Administratorowi danych.
8. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu koordynator zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
9. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Burmistrza, koordynatora, Administratora Systemu Informatycznego oraz pełnomocnika ds. Informacji Niejawnych w Urzędzie.
10. Analiza, o której mowa w ust. 9, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział IX
PRZEPISY KOŃCOWE

§ 29. Pracownik, który:

1. przetwarza w zbiorze danych dane osobowe:
   - do których przetwarzania nie jest upoważniony,
   - których przetwarzanie jest zabronione,
   - niezgodnie z celem stworzenia zbioru danych;
2. udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
3. nie zgłasza Administratorowi danych lub koordynatorowi zbiorów danych podlegających rejestracji;
4. nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
5. uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw
   - podlega odpowiedzialności karnej zgodnie z ustawą o ochronie danych osobowych oraz sankcjami określonymi w kodeksie pracy.

§ 30. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie, zgodnie z art. 31 Ustawy o ochronie danych osobowych. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik **Nr 8** do niniejszej Polityki.

§ 31. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182 ze zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych(Dz. U. Nr 100 poz. 1024).

Załącznik nr 1 do Polityki bezpieczeństwa

.....
(imię i nazwisko)

.....
(stanowiska służbowe)

.....
(nazwa jednostki/komórki organizacyjnej)

OŚWIADCZENIE

Oświadczam, że zapoznałem/am się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi Burmistrza Drawna – Administratora Danych Osobowych i zobowiązuję się do ich stosowania.
Świadomy/a jestem obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania, również po ustaniu zatrudnienia lub zakończenia współpracy.

.....
(miejscowość, data)

.....
(czytelny podpis)

Załącznik nr 2 do Polityki Bezpieczeństwa

Drawno, ...

UPOWAŻNIENIE Nr .....
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 poz. 1182 ze zm.)) z dniem .....

upoważniam Panią/Pana*) .....

zatrudnioną/zatrudnionego

w .....

(nazwa komórki organizacyjnej)

na stanowisku: .....

.....

(zajmowane stanowisko)

do przetwarzania danych osobowych w następujących zbiorach:

1) nazwa zbioru: .....

w zakresie: wprowadzanie/odczyt/modyfikacja/usuwanie/administracja*

2) nazwa zbioru: .....

w zakresie: wprowadzanie/odczyt/modyfikacja/usuwanie/administracja*

3) nazwa zbioru: .....

w zakresie: wprowadzanie/odczyt/modyfikacja/usuwanie/administracja*

Ustalam Panu/Pani następujący zakres odpowiedzialności za ochronę zbioru danych j.w. przed nieupoważnionym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem:

1) zobowiązuję Pana/Panią do przestrzegania postanowień Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
2) zobowiązuję Pana/Panią do stosowania przepisów ustawy przy przetwarzaniu danych osobowych w:
   - systemie informatycznym,
   - kartotekach,
   - skorowidzach,
   - księgach,

- wykazach i innych zbiorach ewidencyjnych*,

3) zobowiązuję Pana/Panią do zachowania w tajemnicy danych osobowych w czasie zatrudnienia w Urzędzie Miejskim w Drawnie oraz po ustaniu zatrudnienia w ramach wykonywanych czynności służbowych.

Upoważnienie wygasa z chwilą ustania Pana/Pani*) zatrudnienia na stanowisku .....
w .....
(nazwa instytucji lub komórki organizacyjnej)

.....
(Podpis Administratora danych osobowych)

... ...
(Data i podpis pracownika)

Niniejsze upoważnienie zostało sporządzone w trzech jednobrzmiących egzemplarzach – każdy na prawach oryginału, które otrzymują:
osoba upoważniona
dział kadr
koordynator.

*) *niepotrzebne skreślić*

Załącznik nr 3 do Polityki Bezpieczeństwa

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*

Data i podpis Administratora Danych Osobowych

.....

Załącznik nr 4 do Polityki Bezpieczeństwa

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

L.p.	Dokładny adres	Referat użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi

Data i podpis Administratora Danych Osobowych

.....

Załącznik nr 5 do Polityki Bezpieczeństwa

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

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania danych	Uwagi

Data i podpis Administratora Danych Osobowych

.....

Załącznik nr 6 do Polityki Bezpieczeństwa

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Struktura zbiorów** *(np. imię i nazwisko, e-mail, telefon itd.)*	**Przepływ danych** (np. wydruk danych z internetu)	**Uwagi**

Data i podpis Administratora Bezpieczeństwa Informacji

.....

Załącznik nr 7 do Polityki Bezpieczeństwa

Raport
z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Miejskim w Drawnie

1. Data:..... godzina: .....

1. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....

5. Podjęte działania:
.....
.....
.....

6. Przyczyny wystąpienia zdarzenia:
.....
.....
.....

7. Postępowanie wyjaśniające:
.....
.....
.....

.....
(data, podpis koordynatora)

Załącznik nr 8 do Polityki Bezpieczeństwa

Wzór umowy powierzenia przetwarzania danych osobowych

Załącznik do umowy Nr.....

Umowa Nr .....

Zawarta w dniu ..... r. w ..... pomiędzy:

.....zwanym w dalszej części niniejszej umowy „Zleceniodawcą" reprezentowanym przez:
..... – Burmistrza Drawna
a
..... .
zwanym w dalszej części niniejszej umowy „Wykonawcą"
reprezentowanym przez:
.....
o następującej treści:

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy Burmistrzem Drawna a ....., Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych, w trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 ze zm.) zwanej dalej „ustawą".
2. Zleceniodawca oświadcza, że powierzone dane zawarte są w zbiorze danych osobowych o nazwie ....., dla którego Burmistrz Drawna jest Administratorem danych osobowych.
3. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych/:
   1) imię i nazwisko,
   2) numer ewidencyjny PESEL,
   3) seria i numer dowodu osobistego,
   4) ..... .
2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług

szczegółowo opisanych w umowie , o której mowa w § 1 ust. 1 i w sposób zgodny z niniejszą Umową.

§ 3

Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się do zachowanie w tajemnicy wszystkich powierzonych lub uzyskanych danych osobowych, także po rozwiązaniu umowy, o której mowa w § 1 ust. 1.
2. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36 – 39 a ustawy, a w szczególności do:
   1) zapewnienia, aby dostęp do danych osobowych przetwarzanych na podstawie umowy, o której mowa w § 1 ust. 1 mieli tylko pracownicy Wykonawcy:
      a) posiadający wydane przez niego imienne upoważnienie do przetwarzania danych osobowych,
      b) którzy podpisali oświadczenie o znajomości przepisów z zakresu ochrony danych osobowych,
   2) prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w związku z wykonywaniem umowy,
   3) do przechowywania (archiwizacji) w swojej siedzibie dokumentów, o których mowa w pkt 1 i 2 przez 5 lat od momentu rozwiązania umowy, o której mowa w § 1 ust. 1.
2. Wykonawca oświadcza, że zgodnie z rozporządzeniem 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. 100, poz. 1024):
   1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
   2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają poziom bezpieczeństwa określony, jako wysoki,
   3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.
3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
   1) wszelkich przypadkach naruszenia przepisów o ochronie danych osobowych,

2) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
3) wszelkich czynności z własnym udziałem w sprawach dotyczących ochrony danych osobowych prowadzonych w szczególności przed Generalnym Inspektorem Ochrony Danych Osobowych, urzedami państwowymi, policją lub przed sądem,
4) każdym nieupoważnionym dostępie do danych osobowych,
5) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.

5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.
6. Na zakończenie kontroli, o których mowa w ust. 5, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
9. Zabrania się Wykonawcy zawierania umów z podwykonawcami w celu realizacji usługi objętej umową, o której mowa w § 1 ust. 1, bez pisemnej zgody Zamawiającego.

§4

Odpowiedzialność Wykonawcy

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§5

Czas obowiązywania Umowy powierzenia

Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia ..... .

§ 6

Warunki wypowiedzenia Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
   1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
   3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

§ 7

Rozwiązanie Umowy

Wykonawca, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 i niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§8

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§9

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego oraz ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2010 r. Nr 113, poz.759 z późn. zm.).

§10

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

§ 11

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

Zleceniodawca Wykonawca

Załącznik Nr 2
do Zarządzenia Nr 36/2016
Burmistrza Drawna z dnia 27 czerwca 2016r.

INSTRUKACJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE MIEJSKIM W DRAWNIE

Rozdział I

Postanowienia ogólne

§ 1. Instrukcja zarządzania systemem informatycznym zwana dalej instrukcją, jest dokumentem określającym zasady oraz procesy zarządzania oraz administrowania systemami informatycznymi Urzędu Miejskiego w Drawnie, w celu bezpiecznego ich przetwarzania.

§ 2. 1. Instrukcja określa zasady i tryb postępowania Administratora danych osobowych oraz wszystkich użytkowników przetwarzających dane osobowe w systemie informatycznym Urzędu Miejskiego w Drawnie.

2. Podstawa prawna:

1) Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 ze zm.)
2) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100 poz. 1024).

§ 3. Ilekroć w instrukcji jest mowa o:

1) Urzędzie – rozumie się Urząd Miejski w Drawnie,
2) Administratorze danych osobowych – rozumie się Burmistrza Drawna,
3) koordynatorze - rozumie się przez to osobę upoważnioną przez Burmistrza Drawna do koordynowania realizacji zadań wynikających z ustawy o ochronie danych osobowych,
4) Administratorze Systemu Informatycznego (ASI) – rozumie się przez to osobę upoważnioną przez Burmistrza Drawna do realizacji zadań związanych z zarządzaniem systemem informatycznym,
5) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narządzi programowych zastosowanych w celu przetwarzania danych osobowych,
6) zabezpieczaniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
7) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
8) zbiorze danych osobowych – rozumie się przez to każdy posiadający strukturę danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
9) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

10) użytkowniku systemu informatycznego - rozumie się przez to pracownika upoważnionego przez Burmistrza Drawna wyznaczonego do przetwarzania danych osobowych,
11) przełożonym użytkownika – rozumie się przez to kierownika referatu, osobę odpowiedzialną za przestrzeganie zasad przetwarzania i ochrony danych osobowych przez podległych mu pracowników.

Rozdział II
Procedury nadawania uprawnień do przetwarzania danych oraz rejestrowania tych uprawnień w systemie informatycznym

§ 4. 1. Każdy pracownik Urzędu zobowiązany jest zapoznać się z ustawą o ochronie danych osobowych, polityką bezpieczeństwa oraz niniejszą instrukcją i stosować jej przepisy na swoim stanowisku pracy.
2. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie ADO do przetwarzania danych osobowych i ma prawo do wykonywania tylko tych czynności, do których została upoważniona.
3. Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na pisemny wniosek przełożonego użytkownika, złożony do Administratora danych. Wzór wniosku stanowi załącznik **nr 1** do niniejszej instrukcji.
4. Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, natomiast jedna kopia zostaje przekazana do akt osobowych pracownika a druga do koordynatora.
5. Ewidencję uprawnień w zakresie dostępu do systemu informatycznego prowadzi Administrator systemów informatycznych na podstawie otrzymanego wniosku i upoważnienia. Wzór ewidencji stanowi załącznik **nr 2** do niniejszej instrukcji.
6. Nadużycie przez użytkownika systemu postanowień niniejszej instrukcji, może stanowić podstawę do pociągnięcia do odpowiedzialności przewidzianej właściwymi przepisami prawa.
7. Użytkownik systemu, który przetwarza dane osobowe zobowiązany jest do zachowania tajemnicy. Tajemnica obowiązuje również po ustaniu zatrudnienia.
8. Użytkownik systemu jest wyrejestrowany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień dostępu do danych osobowych m.in.:
1) ustania zatrudnienia,
2) zmiany zakresu obowiązków,
3) inną utratą uprawnienia.
9. Informację pisemną o ustaniu zatrudnienia, zmianie zakresu obowiązków i utracie uprawnienia, pracownik zatrudniony na stanowisku ds. kadr przekazuje Administratorowi danych z chwilą ich zaistnienia.

§ 5. Naczelną zasadą bezpieczeństwa systemu informatycznego jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym

zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników ma podstawowy wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 6. Dla każdego użytkownika systemu podczas przyznawania uprawnień ASI ustala identyfikator i hasło. Ustanowione hasło ASI przekazuje użytkownikowi systemu w formie pisemnej i ustnej.

Rozdział III
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

§ 7. 1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Osobą odpowiedzialną za prawidłowe funkcjonowanie mechanizmów zawartych w § 5 jest ASI.

§ 8. 1. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
2. Identyfikator składa się z z 6 znaków, z których dwa pierwsze odpowiadają literom imienia a cztery kolejne odpowiadają pierwszym literom nazwiska. W identyfikatorze pomija się polskie znaki diaktryczne.
3. Identyfikator wpisuje się do ewidencji, prowadzonej przez Administratora Systemu Informatycznego, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp, a następnie wprowadzany jest przez ASI do właściwych systemów.
4. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

§ 9. 1. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników.
2. Hasło przydzielone użytkownikowi należy zmienić podczas pierwszego logowania się w systemie informatycznym przetwarzającym dane osobowe.
3. Hasła są zmieniane przez użytkownika lub ASI.
4. W celu zapewnienia wysokiego poziomu bezpieczeństwa hasło musi zawierać co najmniej 8 znaków i zawierać jednocześnie duże i małe litery oraz cyfry lub znaki specjalne.
5. Użytkownik systemu utrzymuje hasło w tajemnicy – również po upływie jego ważności. Jest odpowiedzialny za zachowanie poufności swoich haseł i powinien wprowadzać hasło w taki sposób, który uniemożliwia innym osobom jego poznanie.
6. Hasło użytkownika systemu musi być zmieniane nie rzadziej niż raz na 30 dni. W przypadku gdy użytkownik systemu informatycznego nie korzysta z danego systemu przez okres dłuższy niż 30 dni, hasło musi być zmienione podczas najbliższego ponownego zalogowania.

7. Hasło użytkownika systemu, który utracił uprawnienia dostępu do danych osobowych unieważnia się bezzwłocznie oraz podejmuje inne niezbędne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 10. Użytkownik systemu ponosi odpowiedzialność za czynności wykonane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje i zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia wszelkich starań w celu uniemożliwienia zapoznania się z nimi osób trzecich nawet po ustaniu ich ważności.

§ 11. 1. Identyfikatory i hasła użytkowników powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie osoby uprawnione.
2. Identyfikatory użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem ASI kopercie.
3. W przypadku konieczności awaryjnego użycia loginów i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniałą sytuację w „Dzienniku haseł" znajdującej się w szafie wraz z kopertą, w której znajdują się hasła.
4. Wpis, o którym mowa w ust. 3 powinien zawierać następujące informacje:
   1) imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
   2) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
   3) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.
5. O konieczności oraz okoliczności awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony Administrator danych osobowych oraz koordynator.

Rozdział IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

§ 12. 1. Użytkownik systemu rozpoczynający pracę zobowiązany jest do przestrzegania procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego.
2. Użytkownik systemu przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem.
3. Użytkownik systemu w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:
   1) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwić podgląd osobom nieuprawnionym,
   2) w przypadku przekroczenia 20 minut braku aktywności następuje automatyczna blokada systemu bądź automatyczny wygaszacz ekranu chroniony hasłem.
4. Przy każdorazowym opuszczaniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane osobowe poprzez zabezpieczenie komputera lub wylogowanie się z systemu.

5. Przed wyłączeniem komputera należy bezwzględnie zarchiwizować dane, następnie zakończyć pracę uruchomionych aplikacji, wykonać zamknięcie systemu i sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji (płyty CD, pamięci usb itp.).
6. Użytkownik w pełnym zakresie odpowiada za powierzony sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia sprzętu komputerowego.

Rozdział V
Procedury tworzenia kopii zapasowych i zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 13. 1. W cyklu dziennym kopie wykonywane są w serwerze oraz na odrębnym stanowisku komputerowym pełniącym funkcję archiwum.
2. W razie potrzeby kopie zapasowe wykonywane są przez użytkowników aplikacji na płytach lub na odrębnym stanowisku komputerowym pełniącym funkcję archiwum.
3. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego.

Rozdział VI
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w § 5 pkt 4 rozporządzenia

§ 14. 1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem.
2. Nośniki danych osobowych oraz wydruki powinny być przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych określony w Polityce bezpieczeństwa i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar.
3. Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych.
4. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
5. Przeznaczone do likwidacji urządzenia, dyski oraz inne elektroniczne nośniki informacji, mogące zawierać dane osobowe, pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie, nie później niż po upływie 3 dni.
6. Za skasowanie zbędnych danych lub zniszczenie zbędnych nośników elektronicznych odpowiedzialny jest Administrator Systemu Informatycznego.
7. Kopie zapasowe zbioru danych osobowych przechowywane są w serwerowni.
8. Dostęp do serwerowni mają tylko upoważnieni pracownicy, tj. informatyk i koordynator.
9. Kopie zapasowe przechowuje się przez okres sześciu miesięcy następujących po miesiącu sporządzenia kopii.
10. Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety) są przechowywane na podobnych zasadach, co wydruki

Rozdział VII

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

§ 15. 1. W celu zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych należy zastosować środki bezpieczeństwa na poziomie wysokim.
2. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje informatyk.
3. Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji.
4. Kontrola antywirusowa przeprowadzana jest na wszystkich nośnikach magnetycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
5. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje informatyk, wykorzystując w trakcie pracy moduł programu antywirusowego z aktualną bazą antywirusową.
6. Administrator Systemu Informatycznego ma obowiązek zgłaszać na piśmie Administratorowi Danych Osobowych wszelkie potrzeby lub zauważalne niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.
7. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować informatyka.
8. W przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są zobowiązani bezzwłocznie powiadomić o tym fakcie informatyka, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności.
9. Informatyk jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   - sieci lokalnej;
   - stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

10. Ochrona systemu informatycznego używanego w Urzędzie polega na:
   - ochronie przez identyfikator,
   - ochronie za pomocą hasła,
   - przydzieleniu praw,
   - nadawaniu atrybutów.

11. Bezwzględnie zakazuje się użytkownikom samodzielnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji(magnetycznych, optycznych, urządzeń podłączonych do stacji roboczych). Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody informatyka, po uprzednim sprawdzeniu nośnika informacji przez informatyka pod względem bezpieczeństwa dla systemu informatycznego.

12. Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić Administratora danych oraz informatyka.

Rozdział VIII
Wymagania, które powinien spełniać system informatyczny służący do przetwarzania danych osobowych

§ 16. 1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

2. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3. Zakres działań użytkownika uwzględnia:

- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

4. W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalająca na automatyczne powiadamianie informatyka o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).

5. Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

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

§ 17. 1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

2. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje stosownie do potrzeb informatyk w porozumieniu z Administratorem danych.

3. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada informatyk.

4. Bezwzględnie zabronione jest dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub niedopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.

5. Użytkownik ma obowiązek niezwłocznie powiadomić ASI lub koordynatora o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia bezpieczeństwa danych osobowych.

6. Sprawdzanie poprawności działania programów i narzędzi programowych przeprowadza się w następujący przypadkach:

- zmiany wersji oprogramowania serwera plików,
- zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu,
- zmiany systemu operacyjnego serwera plików,
- zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu,
- wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modernizacji systemu.

7. Przed dokonaniem zmian w systemie Informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:

- poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
- poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty).

8. Poprawność funkcjonowania aplikacji polega na symulacji działania wykonując następujące operacje:

- wprowadzanie danych osobowych,
- edytowania danych osobowych,
- wyszukiwania danych osobowych,
- wydruku danych osobowych.

9. Przegląd przeprowadza projektant nowego systemu w obecności informatyka.

10. Za prawidłowość przeprowadzania przeglądów i konserwacji systemu odpowiada informatyk.

11. Konserwacje oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
12. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.

§ 18. 1. ASI prowadzi „Dziennik systemu informatycznego Urzędu Miejskiego w Drawnie". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku nr 3 do niniejszej instrukcji.
2. Wpisów do dziennika może dokonywać Administrator danych osobowych lub osoby przez niego upoważnione.

Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym
w Urzędzie Miejskim w Drawnie

Wniosek
o nadanie uprawnień w systemie informatycznym

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień

Imię i nazwisko użytkownika	Referat

Opis i zakres uprawnień użytkownika w systemie informatycznym:

.....
.....
.....
.....
.....
.....
.....
.....

Data wystawienia	Podpis bezpośredniego przełożonego użytkownika
	Podpis kierownika Urzędu

Załącznik nr 2
do Instrukcji zarządzania systemem informatycznym
w Urzędzie Miejskim w Drawnie

Ewidencja uprawnień w zakresie dostępu do systemu informatycznego w Urzędzie Miejskim w Drawnie

L p.	Imię i nazwisko użytkownika	Zakres upoważnienia	Identyfikator	Data rejestracji w systemie	Data wyrejestrowania z systemu	Podpis ASI

Załącznik nr 3
do Instrukcji zarządzania systemem informatycznym
w Urzędzie Miejskim w Drawnie

DZIENNIK SYSTEMU INFORMATYCZNEGO URZĘDU MIEJSKIEGO W DRAWNIE

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:
- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania / wnioski	Podpis

Załącznik Nr 3
do Zarządzenia Nr 36/2016
Burmistrza Drawna z dnia 27 czerwca 2016r.

Regulamin określający zasady i procedury korzystania ze sprzętu komputerowego, oprogramowania, sieci teleinformatycznej oraz poczty elektronicznej Urzędu

I. Zasady korzystania ze sprzętu komputerowego.

1. Sprzęt komputerowy powierza się pracownikom wyłącznie w celu wykonywania obowiązków służbowych.
2. W urzędzie zabrania się pracownikom korzystania ze sprzętu komputerowego, do którego pracodawca nie jest uprawniony.
3. Powierzenie sprzętu następuje na podstawie protokołu przekazania sprzętu komputerowego.
4. Zabrania się dokonywania bez autoryzacji ASI zmian w ustawieniach systemowych komputerów, ustawień BIOS-u, ustawień systemu operacyjnego (w tym instalowanie urządzeń), ustawień sieci teleinformatycznej.
5. Zabrania się samodzielnego otwierania obudowy komputera oraz innych części komputerowych (np. monitorów, drukarek, myszy).
6. Uprawnienia do dokonywania czynności, o których mowa w ust. 4 i 5 na warunkach określonych warunkami gwarancji sprzętu, jest ASI.
7. Pracownik, w którego dyspozycji pozostaje sprzęt komputerowy ma obowiązek wyłączyć go po zakończeniu pracy.
8. Korzystanie z nośników danych dopuszczalne jest po wcześniejszym sprawdzeniu ich programem antywirusowym.
9. Zezwala się pracownikom na korzystanie z przenośnego komputera służbowego poza miejscem pracy jedynie za zgodą przełożonego, zachowując obowiązujące w Urzędzie zasady korzystania z oprogramowania.

II. Zasady korzystania z oprogramowania.

1. Zobowiązuję pracowników do korzystania tylko z legalnego oprogramowania wymienionego w ewidencji, za prowadzenie której odpowiedzialny jest ASI.
2. Instalacje oprogramowania na stanowiskach komputerowych mogą być dokonywane z nośników znajdujących się w zasobach Urzędu. Ich instalacja może być dokonywana wyłącznie przez ASI.
3. Pracownik może dokonać tylko autoryzowanej instalacji. Autoryzowanie instalacji następuje po wydaniu zgody przez ASI, zinwentaryzowaniu oprogramowania i dopisaniu go do ewidencji oprogramowania.
4. Oprogramowanie w wersjach testowych lub w jakikolwiek inny sposób ograniczone umowami licencyjnymi może być użytkowane wyłącznie zgodnie z przeznaczeniem i w czasie określonym w umowie licencyjnej.
5. Zabrania się pobierania i kopiowania z Internetu wszelkich utworów, będących przedmiotem ochrony praw autorskich.

6. Naruszenia wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowią poważne naruszenie dyscypliny pracy.

III. Zarządzanie oprogramowaniem.

1. W Urzędzie obowiązuje wyłącznie pisemna forma wszelkich zamówień dotyczących zakupu oprogramowania.
2. Decyzję o zakupie nowego oprogramowania w Urzędzie podejmuje Burmistrza Drawna lub w jego zastępstwie Sekretarz.
3. Pracownicy nie mogą samodzielnie dokonywać zakupu oprogramowania.
4. Za prowadzenie dokumentacji licencyjnej zakupionego oprogramowania odpowiedzialny jest ASI.
5. Nośniki instalacyjne oprogramowania znajdują się w zamkniętej szafie lub na serwerze zasobów, do których dostęp ma tylko ASI. Nośniki oprogramowania nie mogą być przechowywane w żadnym innym miejscu, a w szczególności nie mogą być kopiowane, wypożyczane lub w żaden inny sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.
6. Przypadki instalowania i uruchamiania oprogramowania niedopuszczonego do użycia przez Urząd (w tym np. oprogramowania skopiowanego własnoręcznie z Internetu), w szczególności, gdy jego uruchomienie powoduje działania niedozwolone, po ich potwierdzeniu, będą podlegały szczegółowej analizie i mogą być traktowane jako celowe i świadome działanie zmierzające do zwiększenia ryzyka działania zasobów i sieci teleinformatycznej Urzędu.

IV. Zasady korzystania z sieci komputerowej (teleinformatycznej) i poczty elektronicznej.

1. Do sieci teleinformatycznej może być podłączony wyłącznie sprzęt będący własnością Urzędu, z zastrzeżeniem ust. 2.
2. Inny sprzęt komputerowy podłączany jest wyłącznie za zgodą ASI.
3. Zabrania się samowolnego podłączania do sieci komputerów lub innych urządzeń.
4. O rozdziale adresów IP decyduje ASI.
5. Zabrania się wykorzystywania gniazd elektrycznych sieci teleinformatycznej w celu zasilania innych urządzeń niż komputery i peryferia komputerowe.
6. W celu zapewnienia bezpieczeństwa mechanizmom sieci teleinformatycznej Urzędu oraz dla jej użytkowników Pracownikom zabrania się dokonywania na niej działań o charakterze nielegalnym, a w szczególności:
   1) umieszczania lub uruchamiania programów i innych obiektów niebezpiecznych, w tym „koni trojańskich" lub innych programów realizujących niepożądane lub wrogie działania,
   2) skanowania sieci teleinformatycznej Urzędu,
   3) prowadzenia aktów, włamań itp. i innych czynności związanych z ingerencją w działanie lub zasoby sieci teleinformatycznej Urzędu lub Internetu,
   4) naruszania w jakikolwiek sposób bezpieczeństwa serwerów i ich bezawaryjnej pracy, a zwłaszcza logowania się do serwerów, jeżeli zakres obowiązków tego wymaga,

5) anonimowego wysyłania poczty elektronicznej z sieci teleinformatycznej Urzędu,
6) gromadzenia na stanowisku pracy, tj. stacji roboczej lub na zasobie dyskowym udostępnionym w sieci LAN, w dowolnej cyfrowej formie materiałów lub treści niezgodnych z obowiązującym prawem lub naruszających dobre obyczaje,
7) uruchamiania programów z komputerowych nośników zewnętrznych,
8) rozpowszechniania nielegalnych plików do Internetu, tj. przesyłania zdjęć, filmów, tekstów czy innych formatów plików.

7. Pracownikom zakazuje się umożliwiania osobom postronnym dostępu do sieci teleinformatycznej Urzędu, np. umożliwienia pracy na identyfikatorach i hasłach pracownika.
8. Zabrania się pracownikom Urzędy wykonywania następujących czynności przy użyciu sprzętu i oprogramowania należącego do pracodawcy:
   1) używania poczty elektronicznej Urzędu do celów innych niż służbowe,
   2) logowania się w celach prywatnych lub komercyjnych na stronach WWW czy też uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, komercyjnym itp.,
   3) używania w celach prywatnych lub komercyjnych komunikatorów internetowych w rodzaju Skype, Gadu-Gadu, itp.,
   4) korzystania z serwisów internetowych niezwiązanych z obowiązkami pracownika,
   5) przetwarzania na komputerach materiałów, do których pracodawca nie posiada praw autorskich,
   6) korzystania z serwisów internetowych zawierających treści niecenzuralne lub jakiekolwiek łamiące prawo obowiązujące na terenie Polski.

V. Procedury kontrolne dotyczące komputerowego stanowiska pracy w Urzędzie.

1. Na wniosek Sekretarza ruch w sieci teleinformatycznej Urzędu, generowany przez pracownika, może podlegać monitoringowi z automatycznym zapisem dostępu do stron WWW.
2. Informacje statystyczne potwierdzające : adresy sieciowe, czas dostępu do najczęściej odwiedzanych przez pracowników serwisów internetowych, gromadzonych plików oraz uruchamianych aplikacji mogą:
   1) podlegać analizie i przekazaniu do kierowników referatów,
   2) stanowić podstawę do dalszych kroków podejmowanych na drodze służbowej.