BURMISTRZ OKONKA
ul. Niepodległości 53
64-965 OKONEK

ZARZĄDZENIE NR 100/2012
Burmistrza Okonka
z dnia 6 listopada 2012 r.

w sprawie „Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Okonku" i „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Miejskim w Okonku".

Na podstawie art. 36 ust. 1, 2 i 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3, 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. Wprowadza się „Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Okonku" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2. Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych w Urzędzie Miejskim w Okonku" stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Urzędzie Miejskim w Okonku do przestrzegania zasad i realizacji zadań określonych w załącznikach, o których mowa w § 1 i 2.

§ 4. Wyznacza się Panią Bronisławę Ćwikła – Sekretarza Miasta i Gminy w Okonku na Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Okonku.

§ 5. Wyznacza się Pana Macieja Naus – Informatyka na Administratora Systemu Informatycznego w Urzędzie Miejskim w Okonku.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ OKONKA
Mieczysław Rapta

Załącznik Nr 1 do Zarządzenia Nr 100/2012
Burmistrza Okonka
z dnia 6 listopada 2012 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIEJSKIM W OKONKU

POSTANOWIENIA OGÓLNE

§ 1. **Polityka bezpieczeństwa** została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024). Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 2. Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Okonku.

§ 3. Ilekroć w regulaminie jest mowa o :

1) **Urzędzie** – rozumie się przez to Urząd Miejski w Okonku;
2) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

5) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Burmistrza Okonka, który decyduje o celach i środkach przetwarzania danych osobowych;
10) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)**- rozumie się przez to osobę wyznaczoną przez Burmistrza Okonka, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
11) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę zatrudnioną przez Burmistrza Okonka, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
12) **kierownik komórki organizacyjnej** – rozumie się również samodzielne stanowisko pracy,
13) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Burmistrza Okonka, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;
14) **reprezentancie** - rozumie się przez to osobę uprawnioną do składania oświadczeń woli w imieniu Administratora Danych;

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

Rozdział I
CELE

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

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

1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

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

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

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

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

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

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji - w razie wątpliwości należy kontaktować się z reprezentantem.

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

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

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

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

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

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

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

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

2. Oświadczenia przechowywane są w aktach osobowych pracownika.

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

2. Upoważnienia określone w ust. 1 przechowywane są w aktach osobowych pracownika.

2. Ewidencję osób biorących udział w przetwarzaniu danych osobowych prowadzi stanowisko do spraw kadr.

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

§ 14.1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w instytucjach samorządowych 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 ADO.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozdział V
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

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

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

3. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Urzędu i sieci zewnętrznych (Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi , WiMAX itp.).

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

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

2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.

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

4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są

aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Rozdział VII
UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

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

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

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

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

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane
7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne

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

8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych
9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

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

§ 28.1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

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

§ 29.1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest Burmistrz Okonka lub pracownik posiadający wymagane prawem upoważnienie.

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

§ 30.1. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO.

Rozdział VIII
ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

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

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

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

Rozdział IX
BEZPIECZEŃSTWO FIZYCZNE

§ 33.1 Dane osobowe, które są przedmiotem zainteresowania ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerach i w postaci akt.

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

§ 34.1. Obszar systemów informatycznych w Urzędzie obejmuje wszystkie pomieszczenia w następujących budynkach:

1) budynek A w Okonku przy ul. Niepodległości 53,
2) budynek B w Okonku przy ul. Niepodległości 53,
3) budynek w Okonku przy ul. Kolejowej 18,
4) budynek w Okonku przy ul. Leśnej 46.

§ 35. Pomieszczenia, w których znajdują się systemy informacji winny być:

1) wyposażone w szafy zamykane na klucz umożliwiające przechowywanie dokumentów,
2) zamknięte, jeśli nikt w nich nie przebywa.

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

Dział X
BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

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

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

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

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

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

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

§ 41.1. Elektroniczne bazy danych osobowych są archiwizowane.

2. Kopie są wykonywane na nośnikach magnetycznych.

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

Rozdział XI
KONSERWACJE I NAPRAWY

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

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

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

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

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

Dział XII
PLANY AWARYJNE I ZAPOBIEGAWCZE

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

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

Rozdział XIII
POLITYKA ANTYWIRUSOWA

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

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

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

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

Rozdział XIV
PRZEPISY KOŃCOWE

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

§ 50. W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

BURMISTRZ OKONKA

Mieczysław Rapta

Załącznik Nr 1
do Polityki Bezpieczeństwa Informacji
w Urzędzie Miejskim w Okonku

WZÓR

	OŚWIADCZENIE

Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am/ - się z „Polityką Bezpieczeństwa Informacji w Urzędzie Miejskim w Okonku" oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Okonku.

Jednocześnie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w Urzędzie Miejskim w Okonku oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.

Potwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, ze zm.) oraz zostałem (am) zaznajomiony z przepisami o ochronie danych osobowych.

Równocześnie oświadczam, że zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej związanej z ochroną danych osobowych.

.....
(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

.....
(data i podpis składającego oświadczenie)

Załącznik Nr 2
do Polityki Bezpieczeństwa Informacji
w Urzędzie Miejskim w Okonku

Wzór

	U P O W A Ż N I E N I E **Nr:**

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), w związku z zakresem czynności wynikającym z umowy..... Z dnia ..... I złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych

upoważniam Pana/Panią:

(Imię i nazwisko)

.....

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/ nie informatycznym w ..... (pełna nazwa komórki organizacyjnej) w zbiorze o nazwie: .....
(podać pełną nazwę zbioru).

Powyższe upoważnienie wydaje się na okres .....
(wpisać na jaki okres lub bezterminowo)

Administrator Danych Osobowych

.....

....., dnia 20..... r.

Załącznik Nr 3
do Polityki Bezpieczeństwa Informacji
w Urzędzie Miejskim w Okonku

WZÓR

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych*

L.p.	Imię i nazwisko	Stanowisko	Komórka organizacyjna	Data przeszkolenia	Nr upoważnienia imiennego*	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia

Załącznik Nr 4
do Polityki Bezpieczeństwa Informacji
w Urzędzie Miejskim w Okonku

Wykaz zbiorów danych przetwarzanych w Urzędzie Miejskim w Okonku

Lp	Nazwa zbioru	Zakres przetwarzanych w zbiorze danych o osobach	Inne dane osobowe	System danych T-tradyc. I-inform.	Nazwa Programu 1) forma danych 2) zabezpieczenie informatyczne, 3) bazę danych chroni UPS (Tak/NIE)	Lokalizacja	Zabezpieczenie fizyczne
1.	PODATKI I OPŁATY LOKALNE GMINY OKONEK	nazwiska i imiona adres zamieszkania lub pobytu	powierzchnia: gospodarstwa rolnego, nieruchomości, lasów, dochód z gospodarstwa rolnego, udzielone ulgi i umorzenia podatku, numer identyfikacji podatkowej	I	SIGID-PODATEK ROLNY/LEŚNY NIERUCHOMOŚCI DLA OSÓB FIZYCZNYCH, PODATEK OD NIERUCHOMOŚCI DLA OSÓB PRAWNYCH, PODATEK ROLNY/LEŚNY DLA OSÓB PRAWNYCH, PODATEK OD ŚRODKÓW TRANSPORTOWYCH, PODATEK OD POSIADANIA PSÓW 1) baza plikowa	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 5,7,8	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, zabezp. p.poż.

					2) indywidualne hasło dostępu 3) tak		
2.	URZĄD STANU CYWILNEGO W OKONKU	nazwiska i imiona imiona rodziców data urodzenia adres zamieszkania lub pobytu numer ewidencyjny pesel zawód wykształcenie seria i numer dowodu osobistego	nazwisko: panieńskie, z poprzedniego małżeństwa, rodowe, miejsce i godzina urodzenia, data i numer aktu: urodzenia, małżeństwa, zgonu, nazwisko i imię: ojca, matki, współmałżonka, płeć, stan cywilny, data i miejsce zawarcia małżeństwa, miejsce wystawienia i numer aktu urodzenia żony, męża, data, godzina, miejsce zgonu, odnalezienia zwłok, data zgonu męża matki, nazwisko, imię, adres osoby zgłaszającej zgon, numer aktu zgonu żony, męża, nazwisko i imię rodowe małżonka, nazwisko rodowe matki i ojca mężczyzny, kobiety, adnotacje o rozwodzie, nazwisko po zawarciu małżeństwa: mężczyzny, kobiety, numer i miejsce wydania dowodu osobistego mężczyzny, kobiety, data unieważnienia aktu małżeństwa, urodzenia, zgonu, imię nadane z urzędu, data i numer orzeczenia sądu ustalającego ojcostwo,	I	Technika – APUSC 1) SQL, 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 13	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

			zaprzeczającego ojcostwo, przysposabiającego dziecko, imię i nazwisko osoby przysposabiającej dziecko, zmiana nazwiska dziecka, data rozwiązania poprzedniego małżeństwa, rozwodu,				
3.	DOWODY OSOBISTE GMINY OKONEK	nazwiska i imiona imiona rodziców data urodzenia adres zamieszkania lub pobytu numer ewidencyjny pesel miejsce pracy zawód wykształcenie seria i numer dowodu osobistego	nazwisko rodowe miejsce urodzenia, stan cywilny, imię i nazwisko rodowe współmałżonka, narodowość, obywatelstwo, rysopis, nazwisko i imię dzieci, stopień pokrewieństwa, miejsce i numer sporządzenia aktu urodzenia, małżeństwa,	I	Zdalny dostęp	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 13	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
4.	EWIDENCJA LUDNOŚCI GMINY OKONEK	nazwiska i imiona imiona rodziców data urodzenia adres zamieszkania lub pobytu numer ewidencyjny pesel miejsce pracy zawód wykształcenie seria i numer dowodu osobistego	stan cywilny, nazwisko rodowe, miejsce i numer aktu urodzenia, małżeństwa, stopień wojskowy numer książeczki wojskowej	I	RADIX – ELUD+ 1) SQL, 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 16	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
5.	DODATKI MIESZKANIOWE GMINY OKONEK	nazwiska i imiona data urodzenia adres zamieszkania lub pobytu miejsce pracy	stopień pokrewieństwa, wysokość dochodów		SYGNITY –Dodatki Mieszkaniowe 1) SQL, 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 7	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na

							klucz, , zabezp. p.poż.
6.	SPRZEDAŻ MIENIA KOMUNALNEGO GMINY OKONEK	nazwiska i imiona adres zamieszkania lub pobytu	numer działki, adres i powierzchnia nieruchomości, numer księgi wieczystej, numer aktu notarialnego,	T		ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 30	kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
7.	SYSTEM INFORMACJI OŚWIATOWEJ	data urodzenia numer ewidencyjny pesel miejsce pracy zawód wykształcenie	forma, rodzaj i wymiar zatrudnienia, kwalifikacje zawodowe, wysokość wynagrodzenia brutto,	I	SIO-System Informacji Oświatowej, MEN 1) baza plikowa 2) indywidualne hasło dostępu 3) tak	ul. Leśna 46, 64-965 Okonek	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
9.	DZIENNIK KORESPONDENCJI	nazwiska i imiona adres zamieszkania lub pobytu	adres poczty elektronicznej,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : A Nr pokoju: 10	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

10.	WYKAZ CZŁONKÓW FORMACJI OBRONY CYWILNEJ	nazwiska i imiona data urodzenia adres zamieszkania lub pobytu zawód		T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : A Nr pokoju: 16, 17	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
11.	PLANY ŚWIADCZEŃ OSOBISTYCH NA RZECZ OBRONY I OBRONY CYWILNE	nazwiska i imiona data urodzenia adres zamieszkania lub pobytu miejsce pracy zawód		T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : A Nr pokoju: 16, 17	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
12.	LISTA POBOROWYCH, WYKAZ PRZEDPOBOROWYCH I REJESTR PRZEDPOBOROWYCH	nazwiska i imiona imiona rodziców data urodzenia adres zamieszkania lub pobytu numer ewidencyjny pesel miejsce pracy wykształcenie seria i numer dowodu osobistego	numer książeczki wojskowej, numer księgi orzeczeń lekarskich,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : A Nr pokoju: 16, 17	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
13.	POSTĘPOWANIE W SPRAWACH O WYKROCZENIE	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, miejsce pracy, seria i numer dowodu		I	eMandat em software s.c. 1) baza plikowa 2) indywidualne hasło dostępu 3) Tak	ul. Kolejowa 18/2, 64-965 Okonek Nr pokoju: 7, 8	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

		osobistego, numer telefonu,					
15.	OŚWIADCZENIA MAJĄTKOWE	nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, numer identyfikacji podatkowej, miejsce pracy zawód, seria i numer dowodu osobistego, numer telefonu,	wysokość dochodów, informacje dotyczące posiadania udziałów w spółkach, składniki mienia ruchomego i nieruchomego, miejsce położenia nieruchomości,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : A Nr pokoju: 1, 15	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
16.	REJESTR SKARG I WNIOSKÓW	nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu,		T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : A Nr pokoju: 15	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
17.	NUMERACJA NIERUCHOMOŚCI	nazwiska i imiona, adres zamieszkania lub pobytu,	Położenie nieruchomości, mapa sytuacyjna wysokościowa, akt własności nieruchomości	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 30	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
18.	WYCINKA DRZEW	nazwiska i imiona, adres zamieszkania lub pobytu,	Nr nieruchomości, mapa sytuacyjne, akt własności nieruchomości,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 24	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

19.	REJESTR WNIOSKÓW I WYDANYCH ZEZWOLEŃ NA UTRZYMYWANIE PSA RASY AGRESYWNEJ	nazwiska i imiona, adres zamieszkania lub pobytu,		T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 24	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
20.	REJESTR DECYZJI O WARUNKACH ZABUDOWY I ZAGOSPODAROWANIA TERENU	nazwiska i imiona, adres zamieszkania lub pobytu,	Nr nieruchomości, mapa sytuacyjne, akt własności nieruchomości,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 30	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
21.	PRZEKSZTAŁCENIE PRAWA UŻYTKOWANIA WIECZYSTEGO WE WŁASNOŚĆ	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, seria i numer dowodu osobistego, numer telefonu,	informacje o posiadanej nieruchomości, wysokość opłaty za użytkowanie wieczyste gruntu, informacje o ulgach oraz stanie zaległości i nadpłat,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 30	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
22.	GOSPODARKA NIERUCHOMOŚCIAMI	nazwiska i imiona, adres zamieszkania lub pobytu, numer identyfikacji podatkowej,	informacje o posiadanej nieruchomości, wysokość opłaty za użytkowanie wieczyste gruntu, informacje o ulgach oraz stanie zaległości i nadpłat,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 30	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
23.	KRAJOWY DROGOWY PRZEWÓZ OSÓB	nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu,	informacja o karalności, numer rejestracyjny pojazdu,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki

		numer ewidencyjny pesel, seria i numer dowodu osobistego, numer telefonu,				Budynek : B Nr pokoju: 30	patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
24.	REJESTR OSÓB UBIEGAJĄCYCH SIĘ O PRZYDZIAŁ MIESZKANIA	nazwiska i imiona , data urodzenia, adres zamieszkania lub pobytu, miejsce pracy,	dane osób zamieszkałych w lokalu mieszkalnym, pokrewieństwo,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 28	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
25.	GOSPODARKA ODPADAMI	nazwiska i imiona, adres zamieszkania lub pobytu,	nr nieruchomości, położenie nieruchomości	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 25	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
26.	REJESTR DECYZJI ŚRODOWISKOWYCH	nazwiska i imiona, adres zamieszkania lub pobytu,	Nr nieruchomości, mapa sytuacyjne, akt własności nieruchomości,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 24	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
27.	REJESTR ZGŁASZANYCH WNIOSKÓW DO PLANÓW ZAGOSPODAROWANIA PRZESTRZENNEGO	nazwiska i imiona , adres zamieszkania lub pobytu,	nr działki, nr nieruchomości,	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek : B Nr pokoju: 30	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
28.	ZMIANA IMION I	nazwiska i imiona,		I	RADIX – ELUD+	ul. Niepodległości	Alarm, kontrola dostępu

	NAZWISK	imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, seria i numer dowodu osobistego,			1) SQL, 2) indywidualne hasło dostępu, 3) tak	53, 64-965 Okonek Budynek A Nr pokoju: 13	przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
29.	RÓŻNE OPŁATY NIEPODATKOWE	nazwiska i imiona, adres zamieszkania lub pobytu, numer identyfikacji podatkowej, numer telefonu,		I	EWIDENCJA I DRUKOWANIE FAKTUR, PROGRAM OBSŁUGI KASY, EWIDENCJA DOCHODÓW NIEPRZYPISANYCHE WIDENCJA OPŁAT ZA WIECZYSTE UŻYTKOWANIE 1) baza plikowa, 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 4, 5	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
30.	CZYNSZE	nazwiska i imiona, adres zamieszkania lub pobytu, numer identyfikacji podatkowej, numer telefonu,	wysokość opłat,	I	SIGID - EWIDENCJA I ROZLICZANIE INNYCH OPŁAT 1) baza plikowa, 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 4, 5	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
31.	AKCYZA	nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny pesel, numer identyfikacji		I	SIGID-PODATEK ROLNY/LEŚNY NIERUCHOMOŚCI DLA OSÓB FIZYCZNYCH	ul. Niepodległości 53, 64-965 Okonek Budynek A	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w

		podatkowej, seria i numer dowodu osobistego, numer telefonu,			1) baza plikowa, 2) indywidualne hasło dostępu, 3) tak	Nr pokoju: 5	szafach zamykanych na klucz, , zabezp. p.poż.
32.	SYSTEM KADROWY	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, zawód, wykształcenie, seria i numer dowodu osobistego,	dochody: miejsce pracy lub nauki członków rodziny, dochody członków rodziny ze wszystkich źródeł	I	SIGID - KADRY I PŁACE PRACOWNIKÓW URZĘDU 1) baza plikowa, 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek B Nr pokoju: 18a	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
33.	SYSTEM ROZLICZEŃ Z ZUS	dane identyfikacyjne osoby ubezpieczonej: identyfikator ubezpieczonego, numer PESEL, NIP, seria i numer dokumentu tożsamości, nazwisko ubezpieczonego, pierwsze imię ubezpieczonego, data urodzenia, adres, numer telefonu,	informacje odnośnie wymiaru i wysokości składek, zasiłków chorobowych, niepełnosprawności	I	Prokom-PŁATNIK 1) baza plikowa, 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 4	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
34.	SYSTEM PŁACOWY	identyfikator ubezpieczonego, pesel, nip, nazwisko i imię, data urodzenia, rodzaj dokumentu tożsamości, numer i seria dokumentu tożsamości,	dane rodzinne, informacje o niepełnosprawności, dane o składkach na ubezpieczenie społeczne, wysokość potrąconego podatku dochodowego, informacje o wynagrodzeniu i obciążeniach, absencja w pracy, wysokość zasiłku chorobowego, nazwisko rodowe, imię ojca i matki,	I	SIGID - KADRY I PŁACE PRACOWNIKÓW URZĘDU 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek A Nr pokoju: 4	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.

			miejsce urodzenia, stan cywilny, nagrody i kary, obowiązek wojskowy, numer konta bankowego				
35.	ZAMÓWIENIA PUBLICZNE	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, zawód, wykształcenie, seria i numer dowodu osobistego, nr telefonu, NIP	kwalifikacje osób wykonujących zamówienia publiczne, numery uprawnień, nr rachunku bankowego, informacje na temat zaległości podatkowych, informacje na temat posiadanych środków finansowych	I	PRZETARGI 4 1) baza plikowa , 2) indywidualne hasło dostępu, 3) tak	ul. Niepodległości 53, 64-965 Okonek Budynek B Nr pokoju: 26	Kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
36.	EWIDENCJA RADNYCH	nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, zawód, wykształcenie, miejsce pracy, nr telefonu	-	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek: A Nr pokoju: 1	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
37.	EWIDENCJA SOŁTYSÓW	nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, zawód, miejsce pracy, nr telefonu	-	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek: A Nr pokoju: 1	Alarm, kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz, , zabezp. p.poż.
37.	ARCHIWUM ZAKŁADOWE	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny	Jak przy wszystkich zbiorach	T	Nie dotyczy	ul. Niepodległości 53, 64-965 Okonek Budynek :A i B pomieszczenia na	Alarm w budynku A, w budynku A i B kontrola dostępu przy rozpoczęciu i po zakończeniu pracy, zamki patentowe,

		PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, NIP				poddaszu	wydruki przechowywane w oddzielnym pomieszczeniu zamykanym na klucz, zabezp. p.poż.

BURMISTRZ OKONKA

Mieczysław Rapta

Załącznik Nr 2
do Zarządzenia Nr 100/2012
Burmistrza Okonka
z dnia 6 listopada 2012 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W OKONKU

§ 1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych Urzędzie Miejskim w Okonku, określa:

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

§ 2. Ilekroć w instrukcji jest mowa o :

1) **ustawie** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej *„ustawą”*;
2) **Urzędzie** – rozumie się przez to Urząd Miejski w Okonku
3) **identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) **haśle** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

5) **sieci telekomunikacyjnej** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)
6) **sieci publicznej** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
7) **teletransmisji** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
8) **rozliczalności** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) **integralności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) **raporcie** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) **uwierzytelnianiu** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
13) **Administratorze Danych Osobowych (ADO)** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Burmistrza Okonka, który decyduje o celach i środkach przetwarzania danych osobowych;
14) **Administratorze Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Burmistrza Okonka, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
15) **Administratorze Systemu Informatycznego (ASI), zwanego też Administratorem Systemu** - rozumie się przez to osobę zatrudnioną przez Burmistrza Okonka, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
16) **kierownik komórki organizacyjnej** – rozumie się przez to również samodzielne stanowisko pracy,
17) **użytkowniku systemu informatycznego** - rozumie się przez to upoważnionego przez Burmistrza Okonka, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych.

§ 3.1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Administratora Bezpieczeństwa Informacji.

2. Wzór wniosku stanowi załącznik do niniejszej instrukcji.

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

§ 4.1. Identyfikator składa się z minimum sześciu znaków.

2. W identyfikatorze pomija się polskie znaki diakrytyczne.

3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z ABI nadaje inny identyfikator.

§ 5.1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

3. Zmiana hasła następuje nie rzadziej niż co 30 dni z zastrzeżeniem § 6.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§ 6.1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek kierownika komórki organizacyjnej.

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

3. Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

3) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
4) zawieszenie w pełnieniu obowiązków służbowych,
5) zwolnienie z pełnienia obowiązków służbowych.

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

§ 7. Rozpoczęcie pracy w systemie odbywa się poprzez:

1) przygotowanie stanowiska pracy,
2) włączenie stacji roboczej,
3) wprowadzenie swojego identyfikatora i hasła.

§ 8. Zakończenie pracy w systemie odbywa się poprzez:

1) zamknięcie aplikacji,
2) odłączenie się od zasobów systemowych,
3) zamknięcie systemu operacyjnego,
4) wyłączenie stacji roboczej.

§ 9.1. Zabrania się użytkownikom pracującym w systemie:

1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
3) używania nielicencjonowanego oprogramowania.

§ 10. 1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Administratora Bezpieczeństwa Informacji, a w szczególności:

1) naruszenia bezpieczeństwa systemu informatycznego,
2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. Administratorowi Bezpieczeństwa Informacji zgłasza się w szczególności przypadki:

1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych

i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

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

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

5. Użytkownik sieci i Administrator Systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

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

§ 11.1. Kopie awaryjne tworzy się z następującą częstotliwością:

1) kopie systemu finansowo - księgowego – dwa razy w miesiącu,
2) kopie pozostałe - nie rzadziej niż raz na miesiąc.

2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.

3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

4. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia Administratora Systemu do ich zniszczenia.

§ 12.1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.

2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemu nie rzadziej niż raz na dwa miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.

4. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

§ 13.1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).

§ 14.1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.

2. Urządzenia, o których mowa w ust. 1 przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.

3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.

4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 15.1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu doraźnie.

2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na dwa tygodnie.

3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na dwa tygodnie.

§ 16.1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 17.l. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

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

§ 18. Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

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

§ 20.l. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

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

3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.

§ 21. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie Administratora Bezpieczeństwa Informacji o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator Bezpieczeństwa Informacji może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

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

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

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

§ 24. System powinien umożliwić udostępnienie na piśmie, w zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, a w szczególności:

a) daty pierwszego wprowadzenia danych tej osoby,
b) źródła pochodzenia danych,
c) nazwy użytkownika wprowadzającego dane,
d) informacji - komu, kiedy i w jakim zakresie dane zostały udostępnione,
e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 7, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

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

§ 26. W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926, z późn. zm.) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

Załącznik
Do Instrukcji Zarządzania Systemem Informatycznym Służącym
Do Przetwarzania Danych Osobowych
w Urzędzie Miejskim w Okonku

WZÓR

Dokument Uprawnień Jednostkowych w systemie informatycznym.

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie

DOTYCZY SYSTEMU: .....
(nazwa aplikacji służącej do przetwarzania danych osobowych)

Imię i nazwisko użytkownika:	Wydział/Stanowisko
Pokój nr:	Telefon nr:
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
Podpis Adm. Systemów Informatycznych i data:	Podpis Adm. Bezpieczeństwa Informacji i data