Zarządzenie Nr 159/2012
Burmistrza Miasta i Gminy Opatów
z dnia 18 stycznia 2012 roku

w sprawie ustalenia" Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Opatowie

Na podstawie art. 36 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami) oraz § 3-5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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

Ustala się Politykę bezpieczeństwa i instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Opatowie, zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Miasta i Gminy w Opatowie do stosowania zasad określonych w Polityce bezpieczeństwa.

§ 3

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§4

Traci moc Zarządzenie Nr 119/2007 z dnia 05 listopada 2007 roku Burmistrza Miasta i Gminy Opatów w sprawie wprowadzenia w Urzędzie Miasta i Gminy w Opatowie: Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa przetwarzania danych osobowych.

§5

Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ
Andrzej Chaziecki

Załącznik

do Zarządzenia Nr 159/2012
Burmistrza Miasta i Gminy Opatów
z dnia 18 stycznia 2012 roku

POLITYKA BEZPIECZEŃSTWA I INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY W OPATOWIE

Rozdział I
Postanowienia ogólne
§ 1.

Ilekroć w Polityce bezpieczeństwa jest mowa o:

1) **Administrator Danych Osobowych** – rozumie się przez to Burmistrza Miasta i Gminy Opatów, zwanego dalej Administratorem Danych.
2) **Administrator Bezpieczeństwa Informacji** – rozumie się przez to osobę wyznaczoną przez Burmistrza Miasta i Gminy Opatów, odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, zwaną dalej ABI.
3) **Administrator Systemów Informatycznych** – rozumie się przez to osobę wyznaczoną przez Burmistrza Miasta i Gminy Opatów, odpowiedzialną za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych, zwaną dalej ASI.
4) **Bezpieczeństwo systemu informatycznego** – rozumie się przez to wdrożenie przez Administratora Danych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
5) **Przetwarzanie danych osobowych** – rozumie się przez to wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
6) **Osoba upoważniona** lub **użytkownik systemu** – rozumie się przez to osobę posiadającą upoważnienie wydane przez Administratora Danych lub uprawnioną przez niego osobę i dopuszczoną jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem.
7) **Przełożony użytkownika** – rozumie się przez to kierownika komórki organizacyjnej Urzędu Miasta i Gminy w Opatowie, zwany dalej przełożonym.
8) **Osoba uprawniona** – rozumie się przez to osobę posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.
9) **Użytkownik uprzywilejowany** – rozumie się przez to posiadającego najwyższy stopień uprawnień do zarządzania systemem informatycznym.
10) **Urząd** – rozumie się przez to Urząd Miasta i Gminy w Opatowie

11) **Systemy informatyczne Urzędu** – rozumie się przez to zespoły współpracujących ze sobą urządzeń, programów, procedur gromadzenia i przetwarzania informacji, narzędzi programowych zastosowanych do przetwarzania danych wraz ze zgromadzonymi danymi oraz osobami upoważnionymi do pracy na tych systemach (w tym obsługa techniczna urządzeń), zwane dalej „systemami".

§ 2.

1. Polityka bezpieczeństwa określa tryb postępowania w przypadku gdy:
   a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Miasta i Gminy w Opatowie.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.

§ 3.

1. Administrator Danych swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu.
2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych urzędu,
   b) podejmowania stosownych działań zgodnie z niniejszą Polityką bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   a) niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   d) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
3. Administrator Bezpieczeństwa Informacji prowadzi następujące ewidencje:
   a) ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe (załącznik nr 14),
   b) ewidencję osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych (załącznik nr 12),
   c) ewidencję oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (Załącznik nr 13),

§ 4.

1. W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach urzędu, określa się obszary przetwarzania danych jako:
   a) obiekty, wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są dane (także w postaci tradycyjnej – papierowej),
   b) części obiektów, w których znajdują się informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).

2. Pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:
   a) być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają je pracownicy zatrudnieni przy przetwarzaniu danych,
   b) jeżeli pomieszczenie znajduje się na parterze lub istnieje możliwość podglądu z zewnątrz, ekrany monitorów umieszcza się w sposób uniemożliwiający taki podgląd,
   c) monitory komputerów, na których wykonuje się przetwarzanie danych, powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.
3. Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki:
   a) wyposażenie (meble) w tej części pomieszczenia muszą być tak ustawione, aby uniemożliwić lub istotnie utrudnić dostęp do tego obszaru osobom nieuprawnionym,
   b) monitory komputerów, na których dokonuje się przetwarzania danych, powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.
4. Obszary przetwarzania danych w obiektach i pomieszczeniach urzędu nie mogą być dostępne dla osób nieuprawnionych.
5. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych albo tradycyjne kartoteki, należy w nich stosować szczególne środki ostrożności, w tym:
   a) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu,
   b) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych,
   c) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie przez osoby nieuprawnione,
   d) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione.

Rozdział II
Opis zdarzeń naruszających ochronę danych osobowych

§ 5.

1. Podział zagrożeń mogących spowodować naruszenie ochrony danych osobowych:
   a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
   c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy).
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
f) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
g) stwierdzenie próby modyfikacji lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie,
i) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
j) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
k) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub „bocznej furtki" itp.,
l) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub skopiowanie danych osobowych,
m) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział III
Zabezpieczenie danych osobowych
§ 6.

1. Administrator Danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych urzędu, a w szczególności:
   a) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   b) zapobiegać zabraniu danych przez osobę nieuprawnioną,
   c) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

2. Do zastosowanych środków technicznych należy:
   a) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   b) zabezpieczenie wejścia do pomieszczeń, o których mowa w lit. a,
   c) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   d) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
3. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
   a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   b) przeszkolenie osób, o których mowa w lit. a, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   c) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
4. Niezależnie od niniejszych zasad opisanych w dokumencie Polityka bezpieczeństwa, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych.
5. Wykaz pomieszczeń, w których przetwarzane są dane osobowe, zawiera Załącznik nr 1 do niniejszego dokumentu.

§ 7.

W celu ochrony przed utratą danych w Urzędzie stosowane są między innymi następujące zabezpieczenia:

1) odrębne zasilanie sprzętu komputerowego,
2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach DVD, z których w przypadku awarii odtwarzane są dane,
4) ochrona przed awarią podsystemu dyskowego przez używanie mirroringu dyskowego, uszkodzenie jakiegokolwiek z dysków nie spowoduje utraty danych,
5) zabezpieczenia przed nieautoryzowanym dostępem do baz danych urzędu:
   a) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do ABI z odpowiednim wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby, jakie ma on mieć udostępnione,
   b) w systemie informatycznym urzędu zastosowano podwójną autoryzację użytkownika:
      - pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło,
      - dostęp do wybranej bazy danych urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu,

§ 8.

1. Określa się pozostałe warunki polityki bezpieczeństwa:
   a) zabezpieczenie przed nieuprawnionym dostępem do danych prowadzone jest przez ABI zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,

b) w pomieszczeniu, w którym znajdują się serwery, zamontowany jest czujnik dymu oraz alarm,
c) w pomieszczeniu, w którym znajdują się serwery, zamontowana jest klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
d) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
e) aby dana osoba była zarejestrowana w systemie informatycznym jako użytkownik, muszą być spełnione następujące warunki:
   - musi wykazać się znajomością ustawy o ochronie danych osobowych,
   - musi wykazać się znajomością niniejszej Polityki bezpieczeństwa i uzyskać upoważnienie imienne do przetwarzania danych osobowych (Załącznik nr 4 do niniejszego dokumentu),
   - podpisać indywidualny zakres czynności (Załącznik nr 11 do niniejszego dokumentu),
   - podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (Załącznik nr 7).

2. Zabrania się użytkownikom systemu:
   a) zapisywania indywidualnych haseł dostępu,
   b) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania oprogramowania,
   c) samodzielnego zakupu sprzętu komputerowego lub oprogramowania,
   d) autoryzacji w systemie jako inny użytkownik,
   e) samodzielnego wgrywania oprogramowania,
   f) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych, zawierającej dane, poza obszar jednostki organizacyjnej,
   g) wykorzystywania Internetu do celów innych niż służbowe oraz przeglądania stron o tematyce pornograficznej, nielegalnych stron z kodami aktywacyjnymi do programów lub programami łamiącymi zabezpieczenia programów przed nielegalnym kopiowaniem,
   h) korzystania z czatów internetowych, ściągania plików muzycznych oraz filmów, korzystania z sieci P2P.
3. Odwiedzanie stron internetowych jest monitorowane przez stanowisko do którego zadań należy prowadzenie informatyki urzędu.
4. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu, należy bezzwłocznie unieważnić.
5. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu, nie może być przydzielony innej osobie.
6. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.
7. Dane wyeksportowane z systemu do komputera mogą znajdować się na tym komputerze tylko przez czas niezbędny do ich wykorzystania.
8. Po wykorzystaniu danych, określonych w ust. 7, należy je niezwłocznie usunąć.
9. Danych określonych w ust. 7 nie można udostępniać osobom nieuprawnionym.

Rozdział IV

Procedury związane z zarządzaniem systemami informatycznymi służącymi do przetwarzania danych osobowych

§ 9.

1. Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych:
   1) Przełożony użytkownika będącego pracownikiem Urzędu wnioskuje na piśmie do administratora danych o upoważnienie imienne do przetwarzania danych osobowych dla siebie i swoich pracowników, wniosek stanowi Załącznik nr 2 do niniejszego dokumentu. Załącznikiem do wniosku jest dokument uprawnień jednostkowych, zawierający dokładny opis uprawnień użytkownika (Załącznik nr 3) oraz podpisane przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (Załącznik nr 8). Wniosek wraz z dokumentem uprawnień jednostkowych, oraz podpisane przez użytkownika oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych składa się do ABI.
   2) W przypadku użytkowników niebędących pracownikami Urzędu Miasta i Gminy w Opatowie wniosek przygotowuje kierownik referatu nadzorującego pracę. Wniosek stanowi Załącznik nr 2 do niniejszego dokumentu. Załącznikiem do wniosku jest oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (Załącznik nr 9). Upoważnienie wygasa samoistnie po upływie okresu, na który zostało przydzielone.
   3) Osoby odbywające staż lub praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia (Załącznik nr 10) nadanego przez Administratora oraz oświadczenia (Załącznik nr 8)
   4) ABI bada poprawność przesłanego dokumentu oraz:
      a) w przypadku uwag przekazuje dokument kierownikowi do uzupełnienia (np. gdy użytkownik nie został zapoznany z przepisami o ochronie danych osobowych). Na dokumencie podaje przyczynę odmowy zatwierdzenia dokumentu. Powtarza czynności do czasu uzyskania akceptacji dokumentu przez ABI,
      b) w przypadku braku uwag przygotowuje upoważnienie do przetwarzania danych osobowych dla użytkownika systemu. Upoważnienie przygotowane jest na piśmie w trzech egzemplarzach (Załącznik nr 4).
   5) Administrator podpisuje upoważnienie do przetwarzania danych osobowych i przekazuje do ABI.
   6) ABI rejestruje użytkownika oraz okres, na który upoważnienie zostało nadane w ewidencji osób upoważnionych.
   7) Egzemplarz upoważnienia ABI niezwłocznie przekazuje ASI w celu rejestracji uprawnień użytkownika w systemach informatycznych.
   8) ASI niezwłocznie dokonuje rejestracji uprawnień użytkownika systemu informatycznego, zgodnie z przekazanym upoważnieniem.
   9) ASI przekazuje upoważnienie do ABI.
   10) ABI dokonuje sprawdzenia nadanych użytkownikowi uprawnień.
   11) ABI przechowuje egzemplarz upoważnienia.
   12) Upoważnienie do obsługi systemów informatycznych w zakresie przetwarzania danych jest załącznikiem do akt personalnych pracownika.

13) Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.
14) Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.
15) ABI i ASI są jednocześnie użytkownikami uprzywilejowanymi.

2. Procedura uwierzytelniania użytkownika w systemie informatycznym:
   1) Niepowtarzalny identyfikator oraz pierwsze hasło jest przydzielone użytkownikowi przez ASI po nadaniu uprawnień do przetwarzania danych osobowych.
   2) Pierwsze hasło jest przekazane przez ASI użytkownikowi systemu w formie pisemnej.
   3) Bezpośredni dostęp do danych użytkownik uzyskuje po podaniu identyfikatora i właściwego hasła.
3. Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego:
   1) Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez ASI, gdy uzyskują lub tracą prawo dostępu do systemu, zgodnie z procedurą nadawania/cofania uprawnień do przetwarzania danych osobowych.
   2) Identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez ASI.
   3) Ustanie stosunku pracy powoduje wyrejestrowanie użytkownika przez ASI. o fakcie ustania stosunku pracy ASI jest niezwłocznie informowany przez przełożonego.
   4) Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.
4. Stosowane metody i środki uwierzytelnienia:
   1) w systemie informatycznym stosuje się uwierzytelniania dwustopniowe, na poziomie:
      a) dostępu do sieci lokalnej,
      b) dostępu do aplikacji,
   2) do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła,
   3) hasło dostępu do sieci lokalnej składa się co najmniej z 6 znaków,
   4) hasło na poziomie dostępu do aplikacji składa się z 6 znaków,
   5) hasło nie może być powtórnie użyte,
   6) hasła nie mogą być powszechnie używanymi słowami. w szczególności nie należy jako hasło wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
   7) hasło nie może być ujawnione nawet po utracie przez nie ważności,
   8) zmiana hasła do systemu następuje nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
5. Procedury zarządzania środkami uwierzytelniania:
   1) dla każdej osoby upoważnionej instalowany jest odrębny identyfikator i hasło, tak aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym mogła mieć tylko ta osoba, która poda właściwy identyfikator i hasło,
   2) system wymusi na użytkowniku zmianę swojego hasła, co 30 dni,
   3) system zostanie wyłączony po trzykrotnej próbie nieudanego logowania się.
6. Procedura rozpoczęcia pracy w systemie informatycznym:
   1) W celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania hasła dostępu do systemu.
   2) Podczas pierwszego uwierzytelniania w systemie użytkownik ma obowiązek zmiany hasła.

3) Hasło składa się co najmniej z 6 znaków:
   a) użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 30 dni kalendarzowych,
   b) zabrania się wpisywania hasła lub jego zmiany w obecności innych osób,
   c) hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych,
   d) w przypadku zagubienia hasła użytkownik musi skontaktować się z ASI w celu uzyskania nowego hasła.

7. Procedura zawieszenia/odwieszenia pracy w systemie informatycznym:
   1) Przy każdorazowym opuszczeniu stanowiska komputerowego dopilnować, aby na ekranie nie były wyświetlane dane osobowe.
   2) W celu zawieszenia pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wyrejestrowania się z systemu.
   3) Przed opuszczaniem miejsca pracy na dłuższy czas użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz ekranu, który jest chroniony hasłem.
   4) W celu ponownego uwierzytelnienia w systemie użytkownik odblokowuje pulpit i rozpoczyna pracę w systemie informatycznym, zgodnie z procedurą rozpoczęcia pracy w systemie informatycznym.

   Zabrania się pozostawiania stanowiska komputerowego z uruchomionym systemem, bez kontroli użytkownika.
8. Procedura zakończenia pracy w systemie informatycznym:
   1) W celu zakończenia pracy w systemie informatycznym użytkownik wyrejestrowuje się z programu służącego do obsługi danych osobowych.
   2) Użytkownik zamyka system operacyjny i wyłącza komputer.
9. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:
   1) Kopie zapasowe są tworzone codziennie po zakończeniu dnia pracy. Nośnikiem jest dysk twardy. Kopie zapasowe dzienne są kopiami pełnymi.
   2) Kopie zapasowe tygodniowe są kopiowane na płyty DVD. Płyty DVD z kopiami zapasowymi są przechowywane w pokoju nr 11a w zamkniętej szafie pancernej.
   3) Kopie zapasowe są okresowo sprawdzane pod kątem ich dalszej przydatności.
   4) Po okresie miesiąca kopie tygodniowe podlegają likwidacji poprzez ich fizyczne zniszczenie. Likwidacji dokonuje ABI i/lub ASI.
10. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz wydruków zawierających dane osobowe:
    1) Elektroniczne nośniki informacji:
       a) dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym, zapisane na dyskietkach czy dyskach twardych, nie mogą być wynoszone poza siedzibę urzędu,
       b) po zakończeniu pracy przez użytkowników systemu elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych,
       c) dane osobowe w postaci elektronicznej, po ustaniu ich użyteczności, należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie,
       d) w przypadku uszkodzenia lub zużycia nośnika elektronicznego zawierającego dane osobowe, należy go fizycznie zniszczyć przez spalenie lub rozdrobnienie,

e) urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   - likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   - przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   - naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

2) Kopie zapasowe:
   Kopie zapasowe zbioru danych osobowych są przechowywane w pokoju nr 11a w szafie pancernej.
3) Wydruki:
   a) wszelkie wydruki zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie czasu ich przydatności są niszczone przy użyciu niszczarek,
   b) wydruki zawierające dane osobowe należy, po ich wykorzystaniu, zniszczyć przez pocięcie w niszczarce, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania,
   c) wydruki zawierające dane sporządzane w oparciu o systemy Urzędu podlegają szczególnej ochronie, a w szczególności niedopuszczalne jest:
      - pozostawianie wydruków zawierających dane, z możliwością dostępu do nich osób nieuprawnionych,
      - wyrzucania nieudanych lub próbnych wydruków do kosza.
4) Dane wejściowe do systemu:
   Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach, co wydruki.

11. Środki ochrony przed wirusami komputerowymi oraz oprogramowaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
   1) Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje ASI.
   2) W celu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, Urząd wykorzystuje:
      - oprogramowanie antywirusowe KASPERSKY ANTI_VIRUS Workstations na serwerze,
      - oprogramowanie KASPERSKY ANTI_VIRUS Workstations na stacjach roboczych.
   3) Aktualizacja wyżej wymienionego oprogramowania jest automatyczna. Bazy wirusów są aktualizowane minimum raz w tygodniu.
   4) Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji.
   5) Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

6) Użytkownik systemu importujący dane osobowe do systemu informatycznego z elektronicznego nośnika jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.
7) O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ASI.
8) Po usunięciu wirusa ASI sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
9) Po dokonanej naprawie lub konserwacji należy przeprowadzić proces sprawdzenia pod kątem występowania wirusów.

12. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej:
1) Użytkownikowi systemu zabrania się dokonywania jakichkolwiek zmian konfiguracji w zainstalowanym oprogramowaniu monitorującym wymianę danych na styku tego stanowiska i sieci lokalnej.
2) Ochrona systemu informatycznego używanego w urzędzie polega na:
a) ochronie przez identyfikator,
b) ochronie za pomocą hasła,
c) przydzielaniu praw,
d) ochronie katalogów,
e) nadawaniu atrybutów.

13. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych:
1) W systemie informatycznym odnotowywane są informacje o odbiorcach danych z tego systemu.
2) Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
a) osoby, której dane dotyczą,
b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie,
c) przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
d) podmiotu, któremu powierzono przetwarzanie danych,
e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3) Odnotowanie obejmuje informacje o:
a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
b) zakresie udostępnianych danych,
c) dacie udostępnienia.
4) Obowiązek odnotowania ww. informacji spoczywa na użytkowniku systemu, w tym celu wypełnia on odpowiednie pole w bazie danych osobowych.
5) Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
6) Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.
7) Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje ABI.

14. Procedury wykonywania przeglądów i konserwacji systemu:
1) Systemy informatyczne oraz nośniki informacji służące do przetwarzania danych eksploatowane w Urzędzie podlegają okresowym przeglądom i konserwacjom.
2) Do dokonywania przeglądów i konserwacji uprawniony jest ASI.

3) W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem w celu naprawy innemu podmiotowi pozbawiane są zawartości.
4) W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są uszkadzane w sposób uniemożliwiający odczytanie danych.
5) Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem ABI i/lubASI.

15. Przeglądy i konserwacja urządzeń:
1) Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego wykonywane są w terminach określonych przez producenta sprzętu.
2) Nieprawidłowości ujawnione w trakcie tych działań zostaną niezwłocznie usunięte, a ich przyczyny przeanalizowane i przekazane ABI.
3) Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

16. Sprawdzanie poprawności działania programów i narzędzi programowych:
1) Sprawdzanie poprawności działania programów i narzędzi programowych przeprowadza się w następujących przypadkach:
a) zmiany wersji oprogramowania serwera plików,
b) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
c) zmiany systemu operacyjnego serwera plików,
d) zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu,
e) wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
2) Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:
a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
b) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty).
3) Poprawność funkcjonowania systemu polega na symulacji następujących operacji:
a) wprowadzania danych osobowych,
b) edytowania danych osobowych,
c) wyszukiwania danych osobowych,
d) wydruku danych osobowych.
4) Przegląd zbiorów danych polega na:
a) sprawdzeniu dostępu do zbiorów danych na poziomie użytkowników o różnych prawach dostępu,
b) ocenie stanu zbiorów danych,
c) sprawdzeniu ustawień dostępu dla poszczególnych użytkowników.

5) W przypadku stwierdzenia nieprawidłowości w stanie zbiorów danych lub naruszenia praw dostępu, administrator systemu powiadamia o zaistniałym fakcie ABI, a następnie podejmuje działania zmierzające do usunięcia nieprawidłowości i zidentyfikowania osoby, która doprowadziła do ich powstania.
6) Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiada ASI.

17. Konserwacja oprogramowania:
1) Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
2) 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.
3) Konserwację przeprowadza ASI.

Rozdział V
Kontrola przestrzegania zasad zabezpieczenia danych osobowych
§ 10.

Administrator Danych lub osoba przez niego wyznaczona (ABI) sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

Rozdział VI
Postępowanie w przypadku naruszenia ochrony danych osobowych
§ 11.

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar itp.)

   należy niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.
2. W razie niemożliwości zawiadomienia ABI, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,

5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI,
9) Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji:
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy urzędu,
   b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   c) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych,
   d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza urzędu,
   e) ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego Załącznik nr 5, który powinien zawierać w szczególności:
      - wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
      - określenie czasu i miejsca naruszenia i powiadomienia,
      - określenie okoliczności towarzyszących i rodzaju naruszenia,
      - wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
      - wstępną ocenę przyczyn wystąpienia naruszenia,
      - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
   f) raport, o którym mowa w lit. e, ABI niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności – osobie uprawnionej.
   g) po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
   h) zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.
   i) analiza, o której mowa w lit. h, 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 VII
Monitorowanie zabezpieczeń
§ 12.

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   a) Administrator Danych,

b) Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególną uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   c) kontrolę właściwej częstotliwości zmiany haseł.

Rozdział VIII
Szkolenia
§ 13.

1. Wszyscy pracownicy urzędu mają obowiązek brać udział w szkoleniach.
2. Szkolenia powinny dotyczyć:
   1) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
   2) przedstawienia zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział IX
Inne uregulowania związane z przetwarzaniem danych osobowych – przetwarzanie danych osobowych w zbiorach doraźnych
§ 14.

1. Dostęp do danych osobowych powinien odbywać się poprzez aplikację edytora tekstu, lub gdy zachodzi potrzeba zapisania danych w innym formacie, np. w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione:
   a) uniemożliwi się dostęp do danych osobom nieuprawnionym,
   b) uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,
   c) zabezpieczy się bezpośredni dostęp do danych hasłem.
2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony, lub zniszczyć nośnik.
3. Należy zawiadamiać ABI w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.
4. Należy przetwarzać dane wyłącznie w pokojach stanowiących obszar przetwarzania danych osobowych w systemie informatycznym urzędu.

§ 15.

1. Wprowadza się następujące zasady korzystania z oprogramowania:
   1) Oryginalne dokumenty licencyjne oraz nośniki każdego oprogramowania przechowywane są na stanowisku ABI, w zamkniętej szafie. Nośniki oprogramowania nie mogą znajdować się w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.
   2) Zabrania się użytkownikom wykonywania kopii oprogramowania.
   3) Wszyscy pracownicy zobowiązani są do pracy na legalnym oprogramowaniu oraz otrzymują wyraźny zakaz instalacji i użytkowania oprogramowania pochodzącego ze źródeł innych niż ABI.

4) Konieczne zakupy oprogramowania powinny być konsultowane z ASI.
5) Do podstawowych obowiązków pracownika należy korzystanie z oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych. Zabrania się korzystania z jakiegokolwiek oprogramowania, do którego Urząd nie jest uprawniony.

2. Instalowanie oprogramowania testowego i bezpłatnego dopuszcza się pod warunkiem:
   1) Do instalacji i modyfikacji oprogramowania na stacjach roboczych uprawniony jest wyłącznie ASI.
   2) Na stacjach roboczych może być instalowane tylko oprogramowanie, na które urząd posiada licencję.
   3) Oprogramowanie testowe może być instalowane wyłącznie na wydzielonych stacjach roboczych.
   4) Przed dopuszczeniem do zainstalowania oprogramowania testowego lub bezpłatnego Administrator Bezpieczeństwa Informacji sprawdza i nadzoruje legalność procesu instalacji oprogramowania.
   5) W szczególnych przypadkach dopuszcza się instalowanie na stacji roboczej oprogramowania testowego, wyłącznie za pisemną zgodą ASI.
   6) Oprogramowanie testowe, określone w pkt. 5 odinstalowuje się bezzwłocznie po zakończeniu testowania.
   7) Użytkownik prowadzący test oprogramowania określonego w pkt. 5 informuje ASI o stwierdzonych nieprawidłowościach.

§ 16.

1) Zasadność zakupu sprzętu komputerowego oraz oprogramowania podlega ocenie i akceptacji przez ASI.
2) ASI nadzoruje proces zakupu sprzętu komputerowego oraz oprogramowania.
3) Instalacja sprzętu komputerowego na stanowiskach pracy wykonywana jest przez ASI.
4) Przeniesienia sprzętu do innych pomieszczeń wykonywane będą przez ASI na wniosek Kierownika Referatu. Zabrania się samodzielnego przenoszenia sprzętu przez innych pracowników.
5) Zmiana osoby odpowiedzialnej za powierzony sprzęt musi być zgłoszona przez Kierownika Referatu do ABI.
6) Użytkownicy ponoszą odpowiedzialność materialną za powierzony im sprzęt komputerowy.

Rozdział X
Postanowienia końcowe

§ 17.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi:

1. Windykacja należności podatkowych – WIP+ – załącznik nr 15
2. Zbiór – rejestr ksiąg urodzeń, małżeństw i zgonów w USC – PB_USC – załącznik nr 16
3. Podatek od środków transportowych – POST - załącznik nr 17
4. Łączne zobowiązanie pieniężne – POGRUN+ - załącznik nr 18
5. Ewidencja ludności – ELUD+ - załącznik nr 19

6. Rejestr wyborców WYB+ - załącznik nr 20
7. Ewidencja gruntów i budynków miasta i gminy Opatów – EWOPIS - załącznik nr 21

§18

1) Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2) Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego Załącznik nr 6 do niniejszego dokumentu.
3) Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
4) Orzeczona kara dyscyplinarna wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5) W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.), 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) oraz Rozporządzenia Ministra Sprawiedliwości z dnia 29 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz.U. Nr 100, poz. 1023).

BURMISTRZ
Andrzej Chuniecki

Załącznik nr 1
do Polityki bezpieczeństwa

WZÓR

GRANICE OBSZARÓW PRZETWARZANIA DANYCH ORAZ OSOBY I REFERATY, KTÓRE PRZETWARZAJĄ DANE OSOBOWE

POKÓJ nr ……… – OBSŁUGA programu ………………………………………	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: ………………………………………

POKÓJ nr ……… – OBSŁUGA programu ………………………………………	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: ………………………………………

POKÓJ nr ……… – OBSŁUGA programu ………………………………………	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: ………………………………………

POKÓJ nr ……… – OBSŁUGA programu ………………………………………	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: ………………………………………

Uwaga!

1. Obsługa techniczna urzędu, (sprzątaczki, pracownicy gospodarczy) podpisują oświadczenie, którego wzór stanowi Załącznik nr 8 do Polityki bezpieczeństwa.
2. Osoby odbywające staż lub praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia (Załącznik nr 10) nadanego przez Administratora oraz oświadczenia (Załącznik nr 8).

Załącznik nr 2
do Polityki bezpieczeństwa

WZÓR

....., dnia .....

Nr ...../.....

WNIOSEK
O NADANIE/COFNIĘCIE UPRAWNIEŃ
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) proszę o nadanie/cofnięcie uprawnień dla

Pani/Pana .....

pracownika .....

do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:

.....

na okres od ..... do .....

.....
(podpis wnioskującego)

Załącznik nr 3
do Polityki bezpieczeństwa

WZÓR

DOKUMENT UPRAWNIEŃ JEDNOSTKOWYCH
IMIĘ i NAZWISKO .....

Lp	Nazwa bazy danych	Rodzaj uprawnień [1]	Uwagi

[1] *Skróty stosowane do określenia uprawnień*
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na ekranie
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych

Uwaga! w przypadku praw ograniczonych do określonej części bazy danych należy ograniczenie to podać w polu Uwagi.

Dane aktualne na dzień: .....

....
(podpis pracownika) *(podpis kierownika komórki organizacyjnej)*

Załącznik nr 4
do Polityki bezpieczeństwa

....., dnia .....

WZÓR

UPOWAŻNIENIE IMIENNE NR...../.....
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.)

upoważniam Panią/Pana .....

pracownika Referatu ..... Urzędu Miasta i Gminy w Opatowie do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:

.....

.....

i nadaję identyfikator: .....

ze szczególnym uwzględnieniem zadań zawartych w 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.

Wyżej wymieniona osoba została przeszkolona i zrozumiała treści ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych do niej przepisach wykonawczych.

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień, jest ważne w terminie od..... do....., wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych Urzędu Miasta i Gminy w Opatowie.

Z dniem podpisania niniejszego upoważnienia traci moc udzielone Pani/Panu upoważnienie Nr ...../.....

Administrator Danych Osobowych

.....
(podpis)

Załącznik nr 5
do Polityki bezpieczeństwa

WZÓR

RAPORT
Z NARUSZENIA BEZPIECZEŃSTWA
SYSTEMU INFORMATYCZNEGO
W URZĘDZIE MIASTA I GMINY W OPATOWIE

1. Data: ..... Godzina: .....
2. 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 Administratora Bezpieczeństwa Informacji)

Załącznik nr 6
do Polityki bezpieczeństwa

WZÓR

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Opatowie", przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych

Przyjąłem/am do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i imię	Komórka organizacyjna	Data, podpis

Załącznik nr 7
do Polityki bezpieczeństwa

WZÓR

....., dnia .....

.....
(imię i nazwisko pracownika)
.....
.....
(komórka organizacyjna)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów:
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych stanowiących tajemnicę służbową wynikającą z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.)
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.
2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych.

....
(podpis pracownika) *(podpis złożono w obecności)*

Załącznik nr 8
do Polityki bezpieczeństwa

WZÓR

.....
(imię i nazwisko pracownika)
.....
.....
(komórka organizacyjna)

OŚWIADCZENIE

Ja, niżej podpisany (a), zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam/będę miał (a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Urzędzie Miasta i Gminy w Opatowie **zarówno w trakcie obecnie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia.**

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Miasta i Gminy w Opatowie, wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał (a) danych osobowych ze zbiorów Urzędu Miasta i Gminy w Opatowie

Stwierdzam, 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 (a) z przepisami o ochronie danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

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

.....
(data i podpis przyjmującego oświadczenie)

Załącznik nr 9
do Polityki bezpieczeństwa

WZÓR

.....
(imię i nazwisko pracownika)
.....
.....
(komórka organizacyjna)

OŚWIADCZENIE

Ja, niżej podpisany (a) zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam/będę miał (a) dostęp w związku z wykonywaniem umowy zawartej z Urzędem Miasta i Gminy w Opatowie, zarówno w trakcie trwania umowy, jak i po jej wygaśnięciu lub rozwiązaniu.

Zobowiązuję się do ścisłego przestrzegania warunków ww. umowy, które wiążą się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał (a) danych osobowych ze zbiorów Urzędu Miasta i Gminy w Opatowie w celach niezwiązanych z wykonywaniem tej umowy.

Stwierdzam, 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(a) z przepisami o ochronie danych osobowych.

Przyjmuję do wiążącej wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami oznacza naruszenie warunków umowy zawartej z Urzędem Miasta i Gminy w Opatowie

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

.....
(data i podpis
przyjmującego oświadczenie)

Załącznik nr 10
do Polityki bezpieczeństwa

WZÓR

.....
(miejscowość, data)

UPOWAŻNIENIE NR .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.)

upoważniam

.....
(imię i nazwisko)

zatrudnionego na stanowisku .....
do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

w Urzędzie Miasta i Gminy w Opatowie
(nazwa jednostki organizacyjnej)

Upoważnienie jest ważne w terminie od ..... do .....

Administrator Danych Osobowych

.....
(podpis)

Załącznik nr 11
do Polityki bezpieczeństwa

WZÓR

.....
(nazwa i adres pracodawcy)

INDYWIDUALNY ZAKRES CZYNNOŚCI
OSOBY ZATRUDNIONEJ
PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Imię i nazwisko pracownika: .....

Stanowisko: .....

Nazwa komórki organizacyjnej: Bezpośredni przełożony:

....

Przetwarzanie 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 (art. 7 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.).

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2002 r. Nr 101, poz. 926, z późn. zm.).

Obowiązkiem każdego pracownika Urzędu Miasta i Gminy w Opatowie jest zachowanie tajemnicy państwowej i służbowej, również w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez Urząd. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Dokumentów materialnych (w formie elektronicznej, papierowej itp.) z danymi osobowymi nie można pozostawiać bez dozoru ani udostępniać osobom nieupoważnionym.

Dokumentacji z danymi nie wolno wykorzystywać do celów innych niż służbowe.

Dokumentacji z danymi nie wolno udostępniać nieuprawnionym.

Pracownik musi dopilnować, aby monitor usytuowany był tak, by ekran był niewidoczny dla osób wchodzących do pomieszczenia.

Przy krótkotrwałych przerwach w pracy należy stosować blokady stacji roboczych.

Pracownik może uzyskać dostęp do systemu tylko i wyłącznie jako użytkownik, na swoje hasło.

Oprogramowanie wgrywa tylko i wyłącznie Administrator Systemu Informatycznego, nie wolno tego robić samodzielnie.

Pracownik odpowiada za wykonany wydruk, ponieważ jest jego właścicielem. w przypadku wykonania wydruku z użyciem drukarki sieciowej, jest obowiązany udać się niezwłocznie do pomieszczenia drukarki i przejąć wydrukowany dokument.

Wydrukowane nadmiarowe, niepotrzebne lub błędne dokumenty należy niezwłocznie, trwale zniszczyć.

Wszelkie informacje, w tym w formie tradycyjnej lub na nośnikach przesyłanych pocztą, zawierające

dane osobowe wysyłane poza Urząd, przekazane mogą zostać tylko po zarejestrowaniu przez kancelarię.

Oświadczam, że znana jest mi definicja danych osobowych w rozumieniu art. 6 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. 2002 r. Nr 101, poz. 926 ze zm.), w myśl której za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, z „Polityką bezpieczeństwa i instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Opatowie

Zobowiązuję się, w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji, Administratora Systemu Informatycznego, a po godzinach urzędowania również ochronę obiektu.

Zobowiązuję się przy przetwarzaniu danych osobowych do szczególnej dbałości o zachowanie poufności, integralności i dostępności danych związanych z dokumentami znajdującymi się w obrocie Urzędu Miasta i Gminy w Opatowie także dotyczących danych osobowych pracowników, dokumentacji systemu przetwarzania danych oraz infrastruktury sprzętowo-programowej systemów informatycznych.

Zobowiązuję się, przy przetwarzaniu danych poza systemem informatycznym, do szczególnej dbałości o zachowanie poufności treści dokumentów, które znajdują się w obrocie w urzędu oraz przestrzegania zasad dostępu do danych osobowych.

Za niedopełnienie obowiązków wynikających z niniejszego zakresu czynności pracownik ponosi odpowiedzialność na podstawie przepisów regulaminu pracy, kodeksu pracy oraz ustawy o ochronie danych osobowych.

Oświadczam, że treść niniejszego zakresu jest mi znana i zobowiązuję się do jego przestrzegania.

Wykonano w 3 egzemplarzach.
Potwierdzam odbiór 1 egzemplarza

....., dnia .....

.....
(czytelny podpis pracownika)

Załącznik nr 12
do Polityki bezpieczeństwa

WZÓR

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH URZĘDU MIASTA I GMINY W OPATOWIE

Lp	Imię i nazwisko	Numer upoważ-nienia	Nazwa zbioru	Nazwa identyfikatora	Okres dostępu	Podpis ABI
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						

Dane aktualne na dzień: .....

Sporządził: .....

Załącznik nr 13
do Polityki bezpieczeństwa

WZÓR

EWIDENCJA OŚWIADCZEŃ O ZACHOWANIU W TAJEMNICY DANYCH OSOBOWYCH OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Lp.	Imię i nazwisko	Numer oświadczenia	Data podpisania oświadczenia	Podpis ABI
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

Dane aktualne na dzień: .....

Sporządził: .....

Załącznik nr 14
do Polityki bezpieczeństwa

WZÓR

EWIDENCJA BAZ DANYCH W SYSTEMACH INFORMATYCZNYCH, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

Lp	Nazwa bazy danych	Nazwisko i imię użytkownika	Nazwa identyfikatora	Rodzaj uprawnień (1)	Uwagi
1.					
2.					
3.					

(1) Skróty stosowane do określenia uprawnień
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na ekranie
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych

Uwaga! w przypadku praw ograniczonych do określonej części bazy danych, należy ograniczenie to podać w polu Uwagi.

Dane aktualne na dzień: .....

Sporządził: .....