

Zarządzenie Nr 98/2015

Wójta Gminy Aleksandrów Kujawski

z dnia 16 września 2015 r.

w sprawie ustalenia „Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Aleksandrowie Kujawskim”.

Na podstawie art. 36 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.) 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. z 2004 r., 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 Gminy w Aleksandrowie Kujawskim, zwaną dalej „Polityką bezpieczeństwa”, która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy w Aleksandrowie Kujawskim do stosowania zasad określonych w Polityce bezpieczeństwa.

§ 3

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4

Traci moc Zarządzenie Nr 13/2007 Wójta Gminy Aleksandrów Kujawski z dnia 05 marca 2007 r. w sprawie: podstawowych warunków technicznych i organizacyjnych stosowanych w celu ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Aleksandrowie Kujawskim.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.


WÓJTA
mgr Andrzej Olszewski

Załącznik

do Zarządzenia Nr 98/2015

Wójta Gminy Aleksandrów Kujawski

z dnia 16 września 2015 r.

POLITYKA BEZPIECZEŃSTWA I INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY W ALEKSANDROWIE KUJAWSKIM

§ 1. Określenia i skróty

- 1. Administrator Danych Osobowych** – Wójt Gminy, zwany dalej Administratorem Danych.
- 2. Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Wójta Gminy, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, zwana dalej ABI.
- 3. Administrator Systemów Informatycznych** – osoba wyznaczona przez Wójta Gminy odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych, zwany dalej ASI.
- 4. Bezpieczeństwo systemu informatycznego** – wdrożenie przez Administratora Danych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
- 5. Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- 6. Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez Administratora Danych lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem.
- 7. Przełożony użytkownika** – kierownik komórki wydziału Urzędu Gminy w Aleksandrowie Kujawskim, zwany dalej przełożonym.
- 8. Osoba uprawniona** – posiadająca upoważnienie wydane przez Administratora Danych do wykonywania w jego imieniu określonych czynności.
- 9. Użytkownik uprzywilejowany** – posiadający najwyższy stopień uprawnień do zarządzania systemem informatycznym.
- 10. Urząd** – Urząd Gminy w Aleksandrowie Kujawskim
- 11. Systemy informatyczne Urzędu** – 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. Cele Polityki bezpieczeństwa

1. Polityka bezpieczeństwa określa tryb postępowania w przypadku gdy:
 - 1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
 - 2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub stan jakości komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Gminy w Aleksandrowie Kujawskim
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. Zadania Administratora Bezpieczeństwa Informacji.

1. Administrator Danych swoją decyzją wyznacza ABI danych zawartych w systemach informatycznych Urzędu.
2. ABI realizuje zadania w zakresie ochrony danych, a w szczególności:
 - 1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych urzędu,
 - 2) 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,
 - 3) niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
 - 4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
3. ABI prowadzi następujące ewidencje:
 - 1) ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe (załącznik nr 15),
 - 2) ewidencję osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych (załącznik nr 13),
 - 3) ewidencję oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (załącznik nr 14),

§ 4. Obszary przetwarzania danych

1. W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach urzędu, określa się obszary przetwarzania danych jako:

- 1) obiekty, wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są dane (także w postaci tradycyjnej – papierowej),
 - 2) części obiektów, w których znajdują się informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).
2. Pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:
- 1) być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy zamykają je pracownicy zatrudnieni przy przetwarzaniu danych,
 - 2) jeżeli pomieszczenie znajduje się na parterze lub istnieje możliwość podglądu z zewnątrz, ekrany monitorów umieszcza się w sposób uniemożliwiający taki podgląd,
 - 3) 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:
- 1) wyposażenie (meble) w tej części pomieszczenia muszą być tak ustawione, aby uniemożliwić lub istotnie utrudnić dostęp do tego obszaru 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:
- 1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu,
 - 2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych,
 - 3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich przeglądanie, wykorzystanie przez osoby nieuprawnione,
 - 4) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione.

Rozdział 1

§ 5. Opis zdarzeń naruszających ochronę danych osobowych.

1. Podział zagrożeń:

- 1) 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.
- 2) 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.
- 3) 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:

- 1) 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. ,
- 2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- 3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działania w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- 4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- 5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazuje na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- 6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- 7) stwierdzenie próby modyfikacyjnej lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- 8) stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie,
- 9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
- 10) 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.,
- 11) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub „bocznej furtki” itp.,
- 12) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub skopiowanie danych osobowych,
- 13) 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, płytach CD/DVD/Blu-ray, pamięciach flash, dyskach przenośnych HDD i SSD w formie niezabezpieczonej itp.

Rozdział 2

§ 6. Zabezpieczenia danych osobowych.

1. Administratorem Danych zawartych i przetwarzanych w systemach informatycznych Urzędu jest Wójt Gminy.

2. Administrator Danych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

- 1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
- 2) zapobiegać zabraniu danych przez osobę nieuprawnioną,
- 3) zapobiegać w przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

- 1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
- 2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1,
- 3) szczególne zabezpieczenie centrum przetwarzania danych (zbiór serwerów i urządzeń w serwerowni komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
- 4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
- 5) Wyposażenie pomieszczeń w odpowiednie gaśnice na wypadek pożaru.
- 6) Niszczarek dokumentów.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

- 1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
- 2) przeszkolenie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
- 3) 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 osobę.

5. 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.

6. Wykaz pomieszczeń, w których przetwarzane są dane osobowe, zawiera Załącznik nr 1 do niniejszego dokumentu.

§ 7. Sposoby zabezpieczeń.

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

- 1) odpowiednie odrębne zasilanie sprzętu komputerowego, stosowanie zasilaczy zapasowych UPS na wypadek zaniku zasilania, zakłóceń, przepięć w sieci energoelektrycznej.
- 2) odrębne zasilanie sprzętu w serwerowni Urzędu,

3) ochrona serwerów przed zanikiem zasilania poprzez stosowanie odpowiednich zasilaczy zapasowych UPS,

4) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach CD/DVD, odrębnych dyskach HDD/SDD z których w przypadku awarii odtwarzane są dane,

5) ochrona przed awarią podsystemu dyskowego przez używanie mirroringu dyskowego, uszkodzenie jakiegokolwiek z dysków nie spowoduje utraty danych,

6) zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

- a) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do ABl z odpowiednim wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby, jakie ma 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,
 - pierwszej autoryzacji należy dokonać w momencie uruchamiania komputera na danym stanowisku pracy, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy – uzyskując również dostęp do zasobów jednego z serwerów Urzędu, podając login użytkownika i hasło,
 - dostęp do wybranej bazy danych urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu,

7) zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet:

- a) w zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, urządzenie sprzętowe typu UTM (ang. *unified threat management* – wielofunkcyjna zaporę sieciową), który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu, adres fizyczny MAC i inne parametry. Ściana ogniowa składa się z bezpiecznego specjalnego systemu operacyjnego i filtra pakietów. Ruch pakietów, które firewall przepuszcza, jest określony przez administratora w postaci reguł.
- b) firewall zapisuje do logów systemowych fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Oprócz filtra pakietów (firewall) zastosowano również narzędzie programowe wykrywające obecność wirusów, trojanów, malware, spyware na komputerach pracowników w czasie pracy programów oraz w poczcie elektronicznej i całego ruchu wewnątrz sieci Urzędu.

§ 8. Postanowienia końcowe.

1. Postanowienia:

- 1) zabezpieczenie przed nieuprawnionym dostępem do danych prowadzone jest przez ABl zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,

- 2) w pomieszczeniach, w których znajdują się serwery zamontowane są czujniki dymu,
- 3) w pomieszczeniach, w których znajdują się serwery, zamontowana jest klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
- 4) w pobliżu wejścia do pomieszczeń z serwerami i innymi urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
- 5) 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 5 do niniejszego dokumentu),
 - podpisać indywidualny zakres czynności (Załącznik nr 12 do niniejszego dokumentu),
 - podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (Załącznik nr 8).

2. Zabrania się:

- 1) zapisywania indywidualnych haseł dostępu,
- 2) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania, aktualizowania oprogramowania,
- 3) samodzielnego zakupu sprzętu komputerowego lub oprogramowania,
- 4) autoryzacji w systemie jako inny użytkownik,
- 5) samodzielnego instalowania, konfigurowania oprogramowania,
- 6) w celach innych niż służbowe, wnoszenie dokumentacji, w tym na nośnikach elektronicznych, zawierające dane, poza obszar jednostki organizacyjnej,
- 7) 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,
- 8) korzystania z czatów internetowych, portali społecznościowych, ściągania plików muzycznych oraz filmów, korzystania z sieci P2P.

3. Odwiedzanie stron internetowych jest monitorowane przez ASI.

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. Do wykorzystania danych, określonych w ust. 7, należy je niezwłocznie usunąć.

9. Danych określonych w ust. 7 nie można udostępniać osobom nieuprawnionym.

10. Wszelkie pliki zawierające dane osobowe oraz pozostałe, na których pracuje użytkownik powinny być szczególnie chronione. Użytkownik ma obowiązek zachowania porządku w strukturze folderów, stosowania odpowiednich nazw folderów i plików w celu łatwej identyfikacji ich zawartości, dat modyfikacji, autorstwa itp.

11. Pracownicy Urzędu mają obowiązek korzystania z zasobów sieci wewnętrznej Urzędu poprzez tworzenie kopii swoich plików na zasób sieciowy – domowy każdego użytkownika oraz pilnowanie aktualności i spójności tych zarchiwizowanych danych.

12. Pracownicy powinni ograniczyć do potrzebnego minimum przenoszenie, przesyłanie przez sieć danych pomiędzy swoimi stanowiskami komputerowymi.

Rozdział 3

§ 9. Procedury związane z zarządzaniem systemami informatycznymi służącymi do przetwarzania danych osobowych

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 3 do niniejszego dokumentu. Załącznikiem do wniosku jest dokument uprawnień jednostkowych, zawierający dokładny opis uprawnień użytkownika (Załącznik nr 4) oraz podpisane przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych składa się do ABI.
- 2) W przypadku użytkowników niebędących pracownikami Urzędu wniosek przygotowuje kierownik wydziału nadzorującego pracę. Wniosek stanowi Załącznik nr 3 do niniejszego dokumentu. Załącznikiem do wniosku jest oświadczenie o zachowaniu w tajemnicy danych osobowych zatrudnionych przy przetwarzaniu danych osobowych (Załącznik nr 10). Upoważnienie wygasa samoistnie po upływie okresu, na który zostało przydzielone.
- 3) 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 5).
- 4) Administrator podpisuje upoważnienie do przetwarzania danych osobowych i przekazuje do ABI.
- 5) ABI rejestruje użytkownika na okres, na który upoważnienie zostało nadane w ewidencji osób upoważnionych.
- 6) Egzemplarz upoważnienia ABI niezwłocznie przekazuje ASI w celu rejestracji uprawnień użytkownika w systemach informatycznych.
- 7) ASI niezwłocznie dokonuje rejestracji uprawnień użytkownika systemu informatycznego, zgodnie z przekazanym upoważnieniem.

- 8) ASI przekazuje upoważnienie do ABI.
 - 9) ABI dokonuje sprawdzenia nadanych użytkownikowi uprawnień.
 - 10) ABI przechowuje egzemplarz upoważnienia.
 - 11) Upoważnienie do obsługi systemów informatycznych w zakresie przetwarzania danych jest załącznikiem do akt personalnych pracownika.
 - 12) Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.
 - 13) 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.
 - 14) 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 wyrejestrowani 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. Stosowanie metody i środki uwierzytelnienia:
- 1) w systemie informatycznym stosuje się uwierzytelniania dwustopniowe, na poziomie:
 - dostępu do systemu operacyjnego komputera na stanowisku pracy,
 - dostępu do sieci lokalnej,
 - dostępu do aplikacji, dostępu do zawartości baz danych na serwerze
 - 2) do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła,
 - 3) hasło dostępu do sieci lokalnej składa się co najmniej z 8 znaków, musi zawierać małe i wielkie litery oraz cyfry i znaki specjalne,
 - 4) hasło na poziomie dostępu do aplikacji składa się z 8 znaków, musi zawierać małe i wielkie litery oraz cyfry i znaki specjalne,
 - 5) hasło nie może być powtórnie użyte,
 - 6) hasło nie może zawierać w sobie identyfikatora użytkownika, loginu użytkownika,
 - 7) hasła nie mogą być powszechnie używanymi słowami, w szczególności nie należy jako hasło wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
 - 8) hasło nie może być ujawnione nawet po utracie przez nie ważności,

- 9) 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 użytkownika 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 zobowiązany 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 8 znaków. Hasło zawiera wielkie i małe litery oraz cyfry i/lub znaki specjalne:
 - 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 użytkownik zobowiązany jest 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 opuszczeniem miejsca pracy na dłuższy czas użytkownik zobowiązany 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 wyrejestrówuje 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 przez ASI Urzędu po zakończeniu dnia pracy. Nośnikiem są dyski HDD i/lub płyty DVD. Kopie zapasowe dzienne są kopiami pełnymi.
- 2) Dyski twarde, płyty DVD z kopiami zapasowymi są przechowywane w pokoju nr 5 w metalowej szafie.
- 3) Kopie zapasowe są okresowo sprawdzane pod kątem ich dalszej przydatności.
- 4) Na koniec każdego miesiąca ABI tworzy kopię miesięczną na dysku HDD i/lub płytach DVD.
- 5) Kopie miesięczne są przechowywane przez okres 5 lat.
- 6) Po okresie przechowywania kopie miesięczne podlegają komisyjnej likwidacji poprzez ich fizyczne zniszczenie. W komisji likwidacyjnej biorą udział ABI 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 nośnikach czy dyskach twardej, 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, namagnesowanie 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 5 w szafie metalowej.
- 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 sporządzone w oparciu o systemy Urzędu podlegają szczególnej ochronie, a w szczególności niedopuszczalne jest:

- pozostawienie 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 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 F-Secure Server Security na serwerze,
 - oprogramowanie F-Secure PSB Workstation Security na stacjach roboczych.
- 3) Aktualizacja wyżej wymienionego oprogramowania jest automatyczna. Bazy wirusów są aktualizowane minimum raz dziennie.
- 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 odpowiedzialny jest 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) ASI jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
 - a) sieci lokalnej i sieci publicznej,
 - b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej,

- 2) W celu zabezpieczenia systemu informatycznego przed nieautoryzowanym dostępem do sieci lokalnej, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, Urząd wykorzystuje:
 - a) Firewall sprzętowy na styku sieci lokalnej i sieci publicznej, zaawansowane zabezpieczenie sieci przed niepowołanym dostępem; zawiera m.in. NAT (Network Address Translation), filtry, wykrywanie i zabezpieczenie przed atakami DoS (Denial of Service), alert przez e-mail, Anti-Virusa, Anti-Spam, IDP (Intrusion Detection and Prevention) system IDP wykrywa i blokuje intruzów przed uzyskaniem dostępu do chronionych zasobów.
 - b) Oprogramowanie F-Secure PSB Workstation Security, ochrona www, na stacjach roboczych.
- 3) Użytkownikowi systemu zabrania się dokonywania jakichkolwiek zmian konfiguracji w zainstalowanym oprogramowaniu monitorującym wymianę na dysku na styku tego stanowiska i sieci lokalnej .
- 4) 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,
 - f) szyfrowaniu plików, spakowanych zbiorów plików.

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) Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego, a raport przekazywany tej osobie.

8) Nadzór nad prawidłowością odnotowania 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 pozbawione są zawartości.
- 4) W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są uszkodzane w sposób uniemożliwiający odczytanie danych.
- 5) Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem ASI.

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) wprowadzenia danych osobowych,
 - b) edytowania danych osobowych,
 - c) wyszukiwania danych osobowych,
 - d) wydruku danych osobowych.
- 4) Przegląd danych zbiorów 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, ASI 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 4

§ 10. Kontrola przestrzegania zasad zabezpieczenia danych osobowych

1. ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. ABI dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

Rozdział 5

§ 11. Postępowanie w przypadku naruszenia ochrony danych osobowych

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) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
 - 6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar itp.)
należy niezwłocznie powiadomić o tym fakcie ABI.
2. W razie niemożliwości zawiadomienia ABI, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI należy:

- 1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i 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 ABI:
 - 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 6, 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 ust. 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 przeprowadzonej przez Kierownictwo Urzędu, ABI, 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 6

§ 12. Monitorowanie zabezpieczeń.

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,
 - b) kontrolę ewidencji nośników magnetycznych,
 - c) kontrolę właściwej częstotliwości zmiany haseł.

Rozdział 7

§ 13. Szkolenia.

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 8

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

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 zafalszowanie informacji pochodzących z systemu,
 - c) zabezpieczy się bezpośredni dostęp do danych haseł.

2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na który 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. Ogólne zasady i odpowiedzialność przy instalacji oprogramowania.

1. Wprowadza się następujące zasady korzystania z oprogramowania:

- 1) Oryginalne dokumenty licencyjne oraz nośniki każdego oprogramowania przechowywane są przez ASI w zamkniętej szafie. Nośniki oprogramowania nie mogą znajdować się w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczone 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 przekazanych od informatyka Urzędu.
- 4) Konieczne zakupy oprogramowania powinny być konsultowane z ASI.
- 5) Do podstawowych obowiązków pracownika należy korzystanie z oprogramowania w związku z wykonywaniem 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 ABI 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. Zasady wyposażania i eksploatacji stacji roboczych

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 Wydziału. Zabrania się samodzielnego przenoszenia sprzętu przez innych pracowników.
5. Zmiana osoby odpowiedzialnej za powierzony sprzęt musi być zgłoszona przez Kierownika Wydziału do Informatyka Urzędu.
6. Użytkownicy ponoszą odpowiedzialność materialną za powierzony im sprzęt komputerowy.

Rozdział 9

§ 17. Postanowienia końcowe

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 dokumentacyjnego 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 7 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 ABI.
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 2014 r., poz. 1182 ze zm.) oraz możliwości wniesienia wobec niej sprawy 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 2014 r., poz. 1182 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 28 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).

WÓJT

mgr Andrzej Olszewski

GRANICE OBSZARÓW PRZETWARZANIA DANYCH ORAZ OSOBY KTÓRE PRZETWARZAJĄ DANE OSOBOWE

Pokój nr 102 i 106 – Obsługa programów „Płatnik” , „ Kadry i Płace” „PZU-eRu”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Beata Kostrzewska - Bożena Szudzik

Pokój nr 5 Serwerownia – OBSŁUGA wszystkich programów znajdujących się w Urzędzie	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Zbigniew Woźniak

Pokój nr 14 - OBSŁUGA programów „ Sygnity SR, FA ,Windykacja, program „Karta Dużej Rodziny” „SEPI”, „Empatia”, „KBIG”, „ERIF Info-Monitor”, „KRD”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Angelika Skibińska - Agnieszka Smardzewska

Pokój nr 7 – OBSŁUGA programu „Wyb +” Komputerowy system rejestru wyborców, program „WOW”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: -Agnieszka Błaszak

Pokój nr 7 - OBSŁUGA programu „Źródło” Rejestr dowodów osobistych i PESEL, „ELUD +” Komputerowy rejestr mieszkańców i rejestr zamieszkania cudzoziemców, program „CEIDG”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Agnieszka Błaszak - Ewa Galasińska

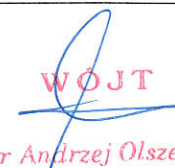
Pokój nr 4 – OBSŁUGA programu „PEFS”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Monika Rolirad

Pokój nr 101, 102 – OBSŁUGA programu „Bestia” „Budżet” „Opłaty lokalne” Egzekucje”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Marek Buczko - Jolanta Niesobska - Szymon Bączalski - Marlena Kuczyńska

Pokój nr 6, 102 – OBSŁUGA programu „Podatki”, Kszob”, „Kasa”, „Auta”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Jacek Modrzejewski - Bożena Biesiada - Joanna Czarnecka - Aneta Niewiadomska - Marlena Kuczyńska - Jolanta Stolarska

Pokój nr 6 – OBSŁUGA programu „SRPP”, SKRIMP”	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Aneta Niewiadomska

Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	
Administrator Danych (Wójt)	Imię i nazwisko - Andrzej Olszewski
Zastępca Wójta	Imię i nazwisko - Halina Rakusiewicz
Sekretarz Gminy	Imię i nazwisko -Arkadiusz Świątkowski
Skarbnik Gminy	Imię i nazwisko - Marek Buczko
Administrator Bezpieczeństwa Informacji	Imię i nazwisko - Alicja Letkiewicz - Sulińska
Radca Prawny	Imię i nazwisko - Marcin Brzdęk
Kierownik	Imię i nazwisko - Malwina Andrusiak
Kierownik	Imię i nazwisko - Maja Majewska
Kierownik	Imię i nazwisko - Tomasz Langner
Kierownik	Imię i nazwisko - Łukasz Korzeniewski


WOJT
 mgr Andrzej Olszewski

Uwaga!

1. Obsługa techniczna urzędu, (sprzątaczkę, 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 11) nadanego przez Administratora oraz oświadczenia (Załącznik nr 8).

OPIS STRUKTUR ZBIORÓW DANYCH

Zbiór danych DOWODY OSOBISTE zawiera następujące pola:

• Imiona i nazwiska,
• Imiona i nazwiska rodowe rodziców,
• Nazwisko rodowe
• Data urodzenia,
• Miejsce urodzenia,
• Numer PESEL,
• Płeć,
• Adres zamieszkania,
• Kod pocztowy,
• Posiadany dotychczasowy dokument tożsamości (seria, nr, nazwa i siedziba wystawcy),
• Przyczyna wystawienia dowodu,
• Data i przyczyna utraty,
• Podpis osoby,
• Fotografia,

WÓJT
mgr Andrzej Olszewski

Zbiór danych EWIDENCJA LUDNOŚCI zawiera następujące pola:

Dane osobowe:
– nazwiska i imiona
– nazwisko rodowe i z poprzedniego małżeństwa
– imiona rodziców,
– data urodzenia,
– miejsce urodzenia,
– akta urodzenia, data i nr USC,
Dane osobowe archiwalne:
– nazwiska i imiona,
– nazwisko rodowe i z poprzedniego małżeństwa,
Adres zamieszkania lub pobytu stałego oraz data zameldowania
Archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania
Adres czasowy oraz czas pobytu czasowego
Archiwalne adresy czasowe oraz okresy pobytów czasowych
Dokument tożsamości
– rodzaj dokumentu,
– seria i numer dowodu,
– wystawca dokumentu,
– rysopis: wzrost, kolor oczu, znaki szczególne;
Numer ewidencyjny PESEL
USC i nr aktu urodzenia
Stan cywilny:
– imię i nazwisko współmałżonka,
– nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
– data zawarcia małżeństwa,
– USC i numer aktu małżeństwa,
– Data wydania i wydający dokument tożsamości,
Stan cywilny archiwalny
– imię i nazwisko małżonka,
– nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
– data zawarcia małżeństwa,
– USC i numer aktu małżeństwa,
Data wydania i wydający dokument tożsamości
Archiwalne dokumenty tożsamości
Obowiązek wojskowy
– czy podlega obowiązkowi,
– nazwa i nr wojskowego dokumentu tożsamości,
– stopień wojskowy,
Data zgonu, USC i numer aktu zgonu
Imiona i nazwiska rodowe
Narodowość
Obywatelstwo (data zmiany, podstawa prawna)
Adnotacje o rozwodzie

Zbiór danych „Podatki” zawiera następujące pola:

Imię i nazwisko podatnika
Adres zamieszkania
Numer NIP
Numer PESEL
Numery ksiąg wieczystych
Numery działek

Zbiór danych „Kadry i Płace” zawiera następujące pola:

Dane osobowe
– imię i nazwisko,
– data urodzenia,
– płeć,
– numer NIP,
– numer PESEL,
– stan cywilny,
– numer i seria dowodu osobistego,
– obywatelstwo,
– przynależność do oddziału NFZ (kasa chorych)
– nazwa banku i numer konta,
– wykształcenie
Dane adresowe
– adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu, kod)
Dane płacowe
– wynagrodzenie,
– składniki płacowe,
– obciążenia komornicze,
– pożyczki

**Zbiór danych „Świadczenia rodzinne i fundusz alimentacyjny”
zawiera następujące pola:**

Dane osobowe
– imię i nazwisko,
– data urodzenia,
– płeć,
– wykształcenie
– numer PESEL,
– stan cywilny,
– numer i seria dowodu osobistego,
– obywatelstwo,
Dane adresowe
– adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu, kod)
Dane (dochód rodziny)
– wynagrodzenie,
– składniki płacowe,
– obciążenia komornicze,
– nazwa banku i numer konta,

Zbiór danych „Opłaty lokalne” zawiera następujące pola:

Dane osobowe
– imię i nazwisko,
– data urodzenia,
– płeć,
– numer PESEL,
– NIP
Dane adresowe
– adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu, kod)

WOJT
mgr Andrzej Olszewski

Załącznik nr 3
do Polityki bezpieczeństwa

....., dnia

Nr/.....

**WNIOSEK
O NADANIE/COFNIĘCIE UPRAWNIENÍ
DO PRZETWARZANIA DANYCH OSOBOWYCH**

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


WOJT
mgr Andrzej Olszewski

Załącznik nr 4

do Polityki bezpieczeństwa

DOKUMENT UPRAWNIEŃ JEDNOSTKOWYCH

IMIĘ I NAZWISKO

Lp	Nazwa bazy danych	Rodzaj uprawnień ¹	Uwagi

¹Skróty 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)

WÓJT
mgr Andrzej Olszewski

Załącznik nr 5

do Polityki bezpieczeństwa

....., dnia

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 Wydziału Urzędu w

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 i 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 w

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

Administrator Danych Osobowych

.....

(podpis)


WOJT
mgr Andrzej Olszewski

RAPOTR
Z NARUSZENIA BEZPIECZEŃSTWA
SYSTEMU INFORMATYCZNEGO
w Urzędzie Gminy w Aleksandrowie Kujawskim

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)

WÓJT
mgr Andrzej Olszewski

Załącznik nr 7

do Polityki bezpieczeństwa

Wykaz osób, które zostały zapoznane z „ Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Aleksandrowie Kujawskim”, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych

Przyjąłem/am do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i imię	Komórka organizacyjna	Data, podpis


WOJT
mgr Andrzej Olszewski

Załącznik nr 8

do Polityki bezpieczeństwa

....., dnia

.....
(imię i nazwisko pracownika)

.....
.....
(adres zamieszkania)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:

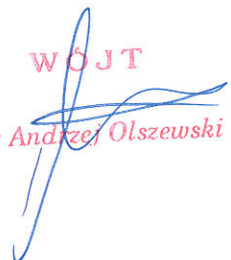
- a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
- b) o ochronie danych osobowych stanowiących tajemnicę służbową wynikającą z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.)
- c) o odpowiedzialności 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)

WÓJT
mgr Andrzej Olszewski



Załącznik nr 9

do Polityki bezpieczeństwa

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 Gminy w Aleksandrowie Kujawskim **,zarówno w trakcie obecnie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia.**

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

Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2014 r. poz. 1182 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.

.....

(nr ewidencyjny, data i podpis

składającego oświadczenie)

.....

(data i podpis przyjmującego oświadczenie)

WOJT
mgr Andrzej Olszewski

Załącznik nr 10

do Polityki bezpieczeństwa

OŚWIADCZENIE

Ja, niżej podpisany (a) zobowiązuję się do zachowania tajemnicy danych osobowych, do których mam/ będę miał (a) dostęp w związku z wykonywaniem umowy zawartej z Urzędem Gminy w Aleksandrowie Kujawskim, 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 Gminy w Aleksandrowie Kujawskim w celach niezwiązanych z wykorzystaniem 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 2014 r., poz. 1182 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 Gminy w Aleksandrowie Kujawskim.

.....
(nr ewidencyjny, data i podpis składającego

oświadczenie)

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

WÓJT
mgr Andrzej Olszewski



Załącznik nr 11

do Polityki bezpieczeństwa

.....

(miejsowość, data)

UPOWAŻNIENIE NR

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182 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 Gminy w Aleksandrowie Kujawskim

(nazwa jednostki organizacyjnej)

Upoważnienie wygasa z chwilą ustania Pana/Pani zatrudnienia w/w stanowisku.

Administrator Danych

.....

(podpis)

WÓJT
mgr Andrzej Olszewski



Załącznik nr 12

do Polityki bezpieczeństwa

.....

.....

.....

(nazwa i adres pracodawcy)

IDYWIDUALNY ZAKRES CZYNNOŚCI

NR ____/____ OSOBY ZATRUDNIONEJ

PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Imię i nazwisko pracownika:

Pracuje na stanowisku

Stanowisko:

od dnia:

Nazwa komórki organizacyjnej:

Bezpośredni przełożony:

.....

.....

Przetwarzanie danych – rozumie się przez to jakiegokolwiek 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 2014 r., poz. 1182 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 2014 r., poz. 1182 ze zm.).

Obowiązkiem każdego pracownika Urzędu Gminy w Aleksandrowie Kujawskim 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 nie widoczny 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. Ustala się czas, po którym system wymusza zmianę hasła, na 30 dni.

Oprogramowanie wgrzywa 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 i 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. 2014 r., poz. 1182 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 Gminy w Aleksandrowie Kujawskim.

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 Gminy w Aleksandrowie Kujawskim, także dotyczących danych osobowych pracowników, dokumentacji i 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 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

Aleksandrów Kujawski, dnia

.....

(czytelny podpis pracownika)

WÓJT
mgr Andrzej Olszewski



Załącznik nr 13

do Polityki bezpieczeństwa

**EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA
DANYCH OSOBOWYCH w SYSTEMACH INFORMATYCZNYCH
URZĘDU GMINY w ALEKSANDROWIE KUJAWSKIM**

Lp.	Imię i nazwisko	Numer upoważnienia	Nazwa zbioru	Nazwa identyfikatora	Okres dostępu	Podpis ABI
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Dane aktualne na dzień:

Sporządził:.....

WÓJT
mgr Andrzej Olszewski

Załącznik nr 14

do Polityki bezpieczeństwa

**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.				

Dane aktualne na dzień:.....

Sporządził:

WÓJT
mgr Andrzej Olszewski



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 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:


WÓJT
mgr Andrzej Olszewski