Zarządzenie Nr 10/2016
Starosty Rypińskiego
z dnia 25 lipca 2016 r.

o zmianie zarządzenia w sprawie ustalenia „Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Rypinie"

Na podstawie art. 36 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) 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. Zmienia się załącznik do Zarządzenia Nr 22/2011 Starosty Rypińskiego z dnia 22 grudnia 2011 r. w sprawie ustalenia „Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Rypinie" w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Starostwa Powiatowego w Rypinie do stosowania zasad określonych w Polityce bezpieczeństwa.

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji i Administratorowi Systemów Informatycznych.

§ 4. Zarządzenie wchodzi w życie z dniem 1 sierpnia 2016 r..

STAROSTA RYPIŃSKI

Starosta Rypiński

mgr inż. Zbigniew Zgórzyński

Załącznik
do Zarządzenia Nr 10/2016
Starosty Rypińskiego
z dnia 25 lipca 2016 r.

POLITYKA BEZPIECZEŃSTWA I INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W RYPINIE

Wprowadzenie

§ 1. Określenia i skróty

1. **Administrator Danych Osobowych** – Starosta Rypiński, zwany dalej Administratorem Danych.
2. **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Starostę Rypińskiego, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, zwana dalej ABI.
3. **Administrator Systemów Informatycznych** – osoba wyznaczona przez Starostę Rypińskiego, 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, zabraniem 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. **Osoba uprawniona** – posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.
8. **Urząd** – Starostwo Powiatowe w Rypinie.
9. **Systemy informatyczne** Starostwa – 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 jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Starostwa Powiatowego w Rypinie
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, którym jest Starosta Rypiński, swoją decyzją w drodze zarządzenia wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu.
2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych urzędu,
   2) prowadzenie rejestru zbiorów danych przetwarzanych przez Administratora Danych zgodnie z art. 36a ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych oraz innych rejestrów czy ewidencji, których obowiązek wynika z ustawy lub aktów wykonawczych do ustawy,
   3) 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,
   4) niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   5) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
3. Administrator Bezpieczeństwa Informacji prowadzi i aktualizuje następujące ewidencje:
   1) ewidencję pomieszczeń, w których przetwarzane są dane osobowe (załącznik nr 1).
   2) ewidencję osób upoważnionych do przetwarzania danych osobowych w Starostwie Powiatowym (załącznik nr 4),
   2) ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe (załącznik nr 6),

§ 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 opuszczają 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. Obszary przetwarzania danych w obiektach i pomieszczeniach urzędu nie mogą być dostępne dla osób nieuprawnionych.
4. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych, należy w nich stosować szczególne środki ostrożności, w tym:
   1) interesanci powinni 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 wykorzystanie przez 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 działanie 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 wskazujące 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 modyfikacji 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 w formie niezabezpieczonej itp.

Rozdział 2

§ 6. Zabezpieczanie danych osobowych

1. Administratorem Danych Osobowych zawartych i przetwarzanych w systemach informatycznych Starostwa

Powiatowego w Rypinie jest Starosta Rypiński.

2. Administrator Danych Osobowych jest obowiązany 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 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) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
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 wychodzącą osobę.

§ 7. Sposoby zabezpieczeń

W celu ochrony przed utratą danych w Starostwie Powiatowym w Rypinie stosowane są między innymi następujące zabezpieczenia:

1) odrębne zasilanie sprzętu komputerowego,
2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych UPS,
3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na serwerze backupu oraz równolegle na taśmach magnetycznych, z których w przypadku awarii odtwarzane są dane,
4) ochrona przed awarią podsystemu dyskowego przez używanie mirroringu dyskowego na serwerach, uszkodzenie jakiegokolwiek z dysków nie spowoduje utraty danych,
5) zabezpieczenia przed nieautoryzowanym dostępem do baz danych urzędu:
   W systemie informatycznym urzędu zastosowano podwójną autoryzację użytkownika:
   - pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do jednostki roboczej, 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,
6) 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, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego.
   b) firewall zapisuje do loginu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów na stronach internetowych oraz w poczcie elektronicznej.

§ 8. Inne postanowienia.

1. Postanowienia:
   1) zabezpieczenie przed nieuprawnionym dostępem do danych prowadzone jest przez ABI zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
   2) w pomieszczeniach, w których znajdują się serwery, zamontowane są urządzenia chłodzące, która

zapewnia właściwą temperaturę powietrza dla sprzętu komputerowego,

3) w serwerowni znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,

2. Zabrania się:
   1) zapisywania indywidualnych haseł dostępu,
   2) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania oprogramowania,
   3) samodzielnego zakupu sprzętu komputerowego lub oprogramowania,
   4) autoryzacji w systemie jako inny użytkownik,
   5) samodzielnego wgrywania oprogramowania,
   6) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych, zawierającej 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 i komunikatorów internetowych, ściągania plików muzycznych oraz filmów, korzystania z sieci P2P.
3. Odwiedzanie stron internetowych jest monitorowane przez Dział Informatyki urzędu.
4. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu, należy bezzwłocznie unieważnić.
5. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.

Rozdział 3

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

1. Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych:
   1) Upoważnienie imienne do przetwarzania danych osobowych nadawane jest pracownikowi przez ABI po podpisaniu umowy o pracę. Upoważnienie przygotowane jest na piśmie w trzech egzemplarzach (Załącznik nr 2). Upoważnienie zawiera jednocześnie oświadczenie o zachowaniu w tajemnicy danych osobowych.
   2) ABI przekazuje informację ASI o nadanym upoważnieniu w celu rejestracji uprawnień użytkownika w systemach informatycznych.
   3) ABI przechowuje egzemplarz upoważnienia.
   4) Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.
   5) 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.
   6) Pracownicy obsługi zatrudnieni przez Starostwo Powiatowe w Rypinie mają prawo do samodzielnego przebywania na terenie pomieszczeń przetwarzania danych po nadaniu uprawnienia (załącznik nr 3).
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) 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) Ustanie stosunku pracy powoduje wyrejestrowanie użytkownika przez ASI. O fakcie ustania stosunku pracy ASI jest niezwłocznie informowany przez przełożonego.
4. Stosowane metody i środki uwierzytelnienia:
   1) w systemie informatycznym stosuje się uwierzytelniania dwustopniowe, na poziomie:

- dostępu do jednostki roboczej,
- dostępu do aplikacji,

2) do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła,
3) hasło dostępu do jednostki roboczej składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne,
4) hasło na poziomie dostępu do aplikacji składa się z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne,
5) hasła nie mogą być powszechnie używanymi słowami. w szczególności nie należy jako hasło wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6) 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) użytkownik dokonuje zmiany swojego hasła, co 30 dni.
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 8 znaków. Hasło zawiera wielkie i małe litery oraz cyfry 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 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.
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 przez ASI Starostwa Powiatowego w Rypinie po zakończeniu dnia pracy. Nośnikami są dyski HDD na serwerze backupu oraz równolegle nośniki magnetyczne.
   2) Płyty DVD z kopiami zapasowymi są przechowywane w pokoju nr 122 w metalowej szafie oraz na mocy porozumienia w serwerowni Urzędu Miasta Rypin. .
   3) Kopie zapasowe są okresowo sprawdzane pod kątem ich dalszej przydatności.
10. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.
    1) Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym, zapisane na płytach optycznych, pamięciach flash czy dyskach twardych, nie mogą być wynoszone poza siedzibę urzędu,
    2) Po zakończeniu pracy przez użytkowników systemu elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych
    3) Dane osobowe w postaci elektronicznej, po ustaniu ich użyteczności, należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie,
    4) W przypadku uszkodzenia lub zużycia nośnika elektronicznego zawierającego dane osobowe, należy

go fizycznie zniszczyć przez spalenie lub rozdrobnienie,

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

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, Starostwo Powiatowe w Rypinie wykorzystuje oprogramowanie antywirusowe:
      – oprogramowanie antywirusowe **F-Secure Server Security** na serwerze,
      – oprogramowanie antywirusowe **F-Secure Client 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) O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ASI.
   7) Po usunięciu wirusa ASI sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
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, Starostwo Powiatowe w Rypinie wykorzystuje:
      a) firewall sprzętowy na styku sieci lokalnej i sieci publicznej, zaawansowane zabezpieczenie sieci przed niepowołanym dostępem; zawiera m.in. NAT (Network Address Translation), alert przez e-mail, Anti-Virusa.
      b) oprogramowanie **F-Secure**, ochrona www, na stacjach roboczych.
   3) Użytkownikowi systemu zabrania się dokonywania jakichkolwiek zmian konfiguracji w zainstalowanym oprogramowaniu monitorującym wymianę danych na styku tego stanowiska i sieci lokalnej jak również instalowania oprogramowania niewiadomego pochodzenia.
   4) Ochrona systemu informatycznego używanego w urzędzie polega na:
      a) ochronie przez identyfikator,
      b) ochronie za pomocą hasła,
      c) przydzielaniu praw,
      d) ochronie katalogów.
13. Procedury wykonywania przeglądów i konserwacji systemu:
   1) Systemy informatyczne oraz nośniki informacji służące do przetwarzania danych eksploatowane w Starostwie Powiatowym w Rypinie 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/lub ASI.

Rozdział 4

§ 10. Kontrola przestrzegania zasad zabezpieczenia danych osobowych

1. 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.
2. ABI dokonuje sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdania w tym zakresie (załącznik nr 5).

Rozdział 5

§ 11. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:
   1) Zabezpieczenia systemu informatycznego,
   2) Zawartości zbioru danych osobowych,
   3) Jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   4) 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 ABI na miejsce naruszenia ochrony danych osobowych 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 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 do sprawozdania, 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 (Staroście), 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.

Rozdział 6

§ 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 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 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 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, (t.j.: Dz. U. z 2016 r. poz. 922) 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 (t.j.: Dz. U. z 2016 r. poz. 922), 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).

STAROSTA
mgr inż. Zbigniew Zgórzyński

GRANICE OBSZARÓW PRZETWARZANIA DANYCH ORAZ OSOBY, KTÓRE PRZETWARZAJĄ DANE OSOBOWE

Nr pokoju	Nazwa zbioru	Imię i nazwisko pracownika
2	EWIDENCJA GRUNTÓW I BUDYNKÓW	Karol Grączewski
6 – 8		Mariusz Wrzesiński Kamil Kaślewicz Danuta Nadratowska
19		Tomasz Sugalski
21		Anna Barańska Bogumiła Betlejewska
108		Zbigniew Stefański Karol Baliński
109		Lech Dobrzeniecki
10	KOMUNIKACJA	Zdzisława Wykpisz
11, 12		Artur Gorczycki Iwona Czachorowska Agata Szocińska Lidia Rutkowska
13		Piotr Pawłowski
14		Katarzyna Lewandowska
103	NIEPDPŁATNE PORADY PRAWNE	Radcy prawni, adwokaci, Organizacje pozarządowe
104	RZECZNIK PRAW KONSUMENTA	Zygmunt Łojko
105 – 107	BUDOWNICTWO	Ewa Muśkiewicz Joanna Kacprzycka Magdalena Meller
110	RYBACTWO	Joanna Dombrowska
119	LEŚNICTWO ŁOWIECTWO REJESTR WODNY	Tomasz Sajnóg Mirosław Murawski
120	GEOLOGIA PRZYRODA	Teresa Mucha

111	Zezwolenia na sprowadzanie zwłok i szczątków ludzkich z zagranicy Ewidencja poborowych	Maria Ostrowska
113	UCZESTNICY PROJEKTÓW EFS	Monika Tomaszewska
114		Krzysztof Wysocki Dominika Więcławska
122		Krzysztof Żebrowski (ASI-informatyk)
207	OŚWIADCZENIA MAJĄTKOWE RADNYCH Rejestr skarg, wniosków i petycji	Agnieszka Donderowicz
209		Honorata Braszka
211	REJESTR KORESPONDENCJI	Natalia Wójcik Honorata Braszka
214 – 216		Barbara Małecka Helena Skomra Małgorzata Kruzińska Małgorzata Winnicka Magdalena Chruściel
217	UCZESTNICY POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO	Dorota Rumińska

STAROSTA
mgr inż. Zbigniew Zgórzyński

UPOWAŻNIENIE NR ...../2016
DO PRZETWARZANIA DANYCH OSOBOWYCH (PDO)

Na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 (Dz. U. z 2016 r. poz. 922), **upoważniam:**

Panią/Pana ..... PESEL .....

do przetwarzania danych osobowych w Starostwie Powiatowym w Rypinie w okresie:

od ..... do ..... .

Upoważnienie wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

Osoba, której dotyczy upoważnienie:

a) ☒* Jest pracownikiem Starostwa Powiatowego w Rypinie .....,
(nazwa komórki organizacyjnej)

b) ☐* Jest stażystą lub praktykantem,

c) ☐* Inne np: personel zewnętrzny dopuszczony do przetwarzania danych w ramach niezbędnych do zrealizowania umowy nr ..... zawartej pomiędzy Starostwem Powiatowym w Rypinie, a .....

.....

*wstawić znak „X",

Upoważnienie dotyczy dostępu do danych osobowych przetwarzanych w formie tradycyjnej (papierowej) oraz danych przetwarzanych w formie elektronicznej w zakresie określonym poniżej.

1. ZAKRES UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH:

UWAGA: Proszę zakreślić znakiem „X" właściwe uprawnienia.

Nazwa zbioru	**Dostęp -wersja papierowa**	**Dostęp -wersja elektroniczna**	**Dodatkowe uwagi** (Np.: zgodnie z zakresem obowiązków wynikających ze stosunku służbowego)
Dane osobowe	☐TAK ☐NIE	☐TAK ☐NIE	
Dane osobowe	☐TAK ☐NIE	☐TAK ☐NIE	
Dane osobowe	☐TAK ☐NIE	☐TAK ☐NIE	
Dane osobowe	☐TAK ☐NIE	☐TAK ☐NIE	
Rejestr korespondencji	☐TAK ☐NIE	☐TAK ☐NIE	

2. POZOSTAŁE UPRAWNIENIA:

1) Dostęp do poczty internetowej: ☐TAK ☐NIE

Nadano adres poczty internetowej (wypełnia ASI): .....

2) Inne uprawnienia (np.: prawo do pracy zdalnej w systemach, indywidualny kod do systemu alarmowego, zezwolenie na wynoszenie kluczy do określonych pomieszczeń poza teren urzędu itp.)

.....

.....

3. Traci moc upoważnienie z dnia ..... r.

4. Oświadczam, że niniejszy zakres uprawnień jest niezbędny do realizowania obowiązków służbowych (wynikających z umowy) przez osobę, której dotyczy upoważnienie.

.....

Data i podpis bezpośredniego przełożonego

5. Osoba została przeszkolona z zakresu ochrony danych osobowych w dniu .....
(obowiązkowo przy nadaniu pierwszego upoważnienia).

.....
Data i podpis osoby prowadzącej/nadzorującej szkolenie

ZATWIERDZAM UPOWAŻNIENIE:	ODBIERAM UPOWAŻNIENIE:
..... Data i podpis ABI	..... Data i podpis ABI
NADANO UPRAWNIENIA W SYSTEMACH	ODEBRANO UPRAWNIENIA W SYSTEMACH
..... Data i podpis Administratora Systemów Informatycznych	..... Data i podpis Administratora Systemów Informatycznych

Przyczyna odebrania niniejszego upoważnienia

.....

.....

.....
(Data i podpis osoby odbierającej Upoważnienie)

ZOBOWIĄZANIE UŻYTKOWNIKA

Oświadczam, że zapoznałam/zapoznałem się z dokumentami „Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Rypinie", wprowadzonymi w Starostwie Powiatowym w Rypinie zarządzeniem Starosty Rypińskiego Nr **...../2016.**

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust 2 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 (t.j.: Dz. U. z 2016 r. poz. 922), również po ustaniu stosunku pracy, oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych wynikających z dokumentacji przetwarzania danych osobowych.

.....
Data i czytelny podpis Pracownika

STAROSTA
mgr inż. Zbigniew Zgorzyński

Załącznik nr 3
do Polityki bezpieczeństwa

UPRAWNIENIE DO SAMODZIELNEGO PRZEBYWANIA NA TERENIE OBSZARU PRZETWARZANIA DANYCH OSOBOWYCH

NUMER UPRAWNIENIA: 01/2016

Na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 (Dz. U. z 2016 r. poz. 922), uprawniam:

Panią/Pana .....

zatrudnioną/zatrudnionego w **Starostwie Powiatowym w Rypinie** do samodzielnego przebywania na terenie pomieszczeń Starostwa Powiatowego w Rypinie o numerach - ...../lub **cały budynek** - stanowiących obszar przetwarzania danych osobowych.

Uprawnienie zostaje nadane na okres **od .... 2016r. do odwołania** w zakresie: **wykonywania prac związanych z utrzymaniem czystości w pomieszczeniach.**

Osoba uprawniona została przeszkolona z zakresu pracy na terenie obszaru przetwarzania danych osobowych w dniu ..... **2016r.**

.....
Data i podpis ABI

ZATWIERDZAM NINIEJSZE UPRAWNIENIE:	ODBIERAM UPRAWNIENIE:
.....	.....
Data I Podpis ABI	Data I Podpis ABI

ZOBOWIĄZANIE OSOBY UPRAWNIONEJ

Oświadczam, że jestem w pełni świadoma/y, iż zakres mojego uprawnienia do przebywania na terenie obszaru przetwarzania danych osobowych nie obejmuje prawa do przetwarzania danych osobowych, w tym do zapoznawania się z ich treścią. W trakcie wykonywania przeze mnie czynności, do których zostałam/zostałem uprawniona/y, na terenie obszaru przetwarzania danych osobowych, ponoszę odpowiedzialność za bezpieczeństwo dokumentów i sprzętu znajdującego się w tych pomieszczeniach.

Zobowiązuje się do zachowania w tajemnicy informacji o danych osobowych i sposobach ich zabezpieczeń, zgodnie z art. 39 ust 2 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 (Dz. U z 2016 r. poz. 922), również po ustaniu nadanego mi uprawnienia.

.....
Data i czytelny podpis osoby uprawnionej

STAROSTA
mgr inż. Zbigniew Zgórzyński

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W RYPINIE

Lp.	Imię i nazwisko	Numer upoważnienia	Nazwa zbioru	Okres upoważnienia	
				Od	Do
1.	Tomasz Sugalski		EWIDENCJA GRUNTÓW I BUDYNKÓW		
2.	Lech Dobrzeniecki				
3.	Anna Barańska				
4.	Bogumiła Betlejewska				
5.	Danuta Nadratowska				
6.	Zbigniew Stefański				
7.	Mariusz Wrzesiński				
8.	Karol Grączewski				
9.	Kamil Kaślewicz				
10.	Karol Baliński				
11.	Maria Ostrowska		1.Zezwolenia na sprowadzanie zwłok i szczątków ludzkich z zagranicy. 2. Ewidencja poborowych		
12.	Ewa Muśkiewicz		BUDOWNICTWO		
13.	Joanna Kacprzycka				
14.	Magdalena Korzepa				
15.	Zdzisława Wykpisz		KOMUNIKACJA		
16.	Artur Gorczycki				
17.	Iwona Czachorowska				
18.	Katarzyna Lewandowska				
19.	Agata Szocińska				
20.	Piotr Pawłowski				
21.	Lidia Rutkowska				
22.	Teresa Mucha		RYBACTWO		
23.	Joanna Dombrowska				
	Teresa Mucha		1. REJESTR WODNY 2. GEOLOGIA		
24.	Tomasz Sajnóg				
	Teresa Mucha		1. LEŚNICTWO 2. ŁOWIECTWO 3. PRZYRODA		
25.	Mirosław Murawski				

26.	Monika Tomaszewska		UCZESTNICY PROJEKÓW EFS		
27.	Krzysztof Wysocki				
28.	Dominika Więcławska				
29.	Natalia Wójcik		REJESTR KORESPONDENCJI		
30.	Honorata Braszka				
31.	Agnieszka Donderowicz		1.OŚWIADCZENIA MAJĄTKOWE RADNYCH 2. REJESTR SKARG WNIOSKÓW I PETYCJI		
32.	Dorota Rumińska		UCZESTNICY POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO		
33.	Zygmunt Łojko		RZECZNIK PRAW KONSUMENTA		
	Radcy prawni Adwokaci		NIEODPŁATNE Pporady PRAWNE		
	Krzysztof Żebrowski (ASI-informatyk)				

Dane aktualne na dzień: .....

Sporządził: .....

STAROSTA

mgr inż. Zbigniew Zgórzyński

SPRAWOZDANIE ZE SPRAWDZENIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

....

oznaczenie administratora danych (pieczątka z adresem siedziby)

imię i nazwisko ABI

okres sprawdzenia od __ - __ - ____ do __ - __ - ____

1. Przedmiot i zakres sprawdzenia.

.....

.....

2. Wykaz osób biorących udział w sprawdzeniu.

Lp.	imię i nazwisko	stanowisko służbowe

3. Wykaz czynności podjętych w toku sprawdzenia.

1.	
2.	
3.	
4.	

4. Opis stanu faktycznego.

.....

.....

.....

5. Stwierdzone przypadki naruszenia przepisów z informacją o działaniach przywracających stan zgodny z prawem.

Lp.	opis uchybienia / zagrożenia *	planowane / podjęte * działanie naprawcze

6. Wykaz załączników do sprawozdania wraz z informacją o formie (papierowa / elektroniczna) ich sporządzenia.

Lp.	Załącznik	forma utrwalenia	ilość

.....
data i miejsce podpisania

.....
podpis ABI **

STAROSTA
mgr inż. Zbigniew Zgórzyński

*niewłaściwe skreślić
**dodatkowo zaparafować każdą ze stron sprawozdania

Załącznik
do sprawozdania

RAPORT
Z NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO W STAROSTWIE POWIATOWYM W RYPINIE

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:

.....

.....

.

STAROSTA

mgr inż. Zbigniew Zgórzyński

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

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

Lp	Nazwa bazy danych	Nazwisko i imię użytkownika	Rodzaj uprawnień [1]
1.	EWIDENCJA GRUNTÓW I BUDYNKÓW	Karol Grączewski	P
		Kamil Kaślewicz	P
		Danuta Nadratowska	P
		Karol Baliński	P
		Lech Dobrzeniecki	P
		Anna Barańska	W
		Bogumiła Betlejewska	W
		Mariusz Wrzesiński	ZAPN
		Zbigniew Stefański	P
		Tomasz Sugalski	P
2.	KADRY I PŁACE	Małgorzata Winnicka	W
		Honorata Braszka	M
3.	PŁATNIK	Małgorzata Winnicka	WPA
4.	DECYZJA – SYSTEM WYDAWANIA I REJESTRACJI DECYZJI BUDOWLANYCH	Ewa Muśkiewicz	W
		Joanna Kacprzycka	W
		Magdalena Meller	W
5.	CEPIK, EST – REJESTRACJA POJAZDÓW	Zdzisława Wykpisz	P
		Artur Gorczycki	P
		Iwona Czachorowska	P
		Lidia Rutkowska	P
		Piotr Pawłowski	P
		Katarzyna Lewandowska	P
		Agata Szocińska	P

[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

Dane aktualne na dzień: .....

STAROSTA
mgr inż. Zbigniew Zgorzyński

Sporządził: .....

Załącznik nr 7
do Polityki bezpieczeństwa

Wykaz osób
zapoznanych z „Polityką bezpieczeństwa i instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Rypinie"

Przyjąłem/am do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i imię	Komórka organizacyjna	Data, podpis
Tomasz Sugalski	Wydział Geodezji, Kartografii, Katastru i Nieruchomości	
Lech Dobrzeniecki		
Anna Barańska		
Bogumiła Betlejewska		
Danuta Nadratowska		
Zbigniew Stefański		
Mariusz Wrzesiński		
Karol Grączewski		
Kamil Kaślewicz		
Karol Baliński		
Zdzisława Wykpisz	Wydział Komunikacji i Dróg	
Artur Gorczycki		
Iwona Czachorowska		
Katarzyna Lewandowska		
Agata Szocińska		
Piotr Pawłowski		
Lidia Rutkowska		
Monika Tomaszewska	Wydział Edukacji, Promocji i Rozwoju	
Krzysztof Wysocki		
Dominika Więcławska		

Ewa Muśkiewicz	Wydział Architektury i Budownictwa	
Joanna Kacprzycka		
Magdalena Korzepa		
Teresa Mucha	Wydział Rolnictwa, Leśnictwa, Ochrony Środowiska i Gospodarki Wodnej	
Joanna Dombrowska		
Tomasz Sajnóg		
Mirosław Murawski		
Barbara Małecka	Wydział Finansowy	
Helena Skomra		
Małgorzata Kruzińska		
Małgorzata Winnicka		
Magdalena Chruściel		
Marianna Czachorowska		
Honorata Braszka	Wydział Spraw Obywatelskich i Zdrowia	
Maria Ostrowska		
Krzysztof Żebrowski		
Natalia Wójcik		
Dorota Rumińska	Samodzielne stanowisko ds. zamówień publicznych	
Agnieszka Donderowicz	Samodzielne stanowisko ds. obsługi organów powiatu	
Zygmunt Łojko	Powiatowy Rzecznik Konsumentów	

STAROSTA

mgr inż. Zbigniew Zgórzyński