Załącznik Nr 1
do Zarządzenia Nr 33/2012
Starosty Myśliborskiego
z dnia 23 maja 2012 r.

POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
W STAROSTWIE POWIATOWYM
W MYŚLIBORZU

SPIS TREŚCI:

ZAŁĄCZNIKI:

Załącznik nr 1.	Wykaz zbiorów danych osobowych wraz nazwą systemu służącego do ich przetwarzania oraz ich strukturą
Załącznik nr 2.	Wykaz obszarów, w których przetwarzane są dane osobowe
Załącznik nr 3.	Wzór upoważnienia do pobierania kluczy i dostępu do pomieszczenia serwerowni
Załącznik nr 4.	Wzór wniosku o wydanie upoważnienia do przetwarzania danych osobowych
Załącznik nr 5	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 6	Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 7.	Wzór oświadczenia o zapoznaniu się z dokumentacją dotyczącą ochrony danych osobowych
Załącznik nr 8.	Wzór ewidencji osób, które zostały zapoznane z dokumentacją dotyczącą ochrony danych osobowych
Załącznik nr 9.	Wzór zgłoszenia z naruszenia bezpieczeństwa danych osobowych
Załącznik nr 10	Wzór raportu ze zgłoszenia naruszenia bezpieczeństwa danych osobowych
Załącznik nr 11.	Wzór wniosku o udostępnienie danych ze zbioru danych osobowych
Załącznik nr 12.	Wzór ewidencji udostępnienia danych osobowych

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa przetwarzania danych osobowych w sposób tradycyjny oraz w systemach informatycznych w Starostwie Powiatowym w Myśliborzu. Opisane reguły określają granice dopuszczalnego zachowania wszystkich pracowników biorących udział w przetwarzaniu danych osobowych w urzędzie.

Potrzeba jego opracowania wynika z § 3 i 4 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, póz. 1024).

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.

Polityka bezpieczeństwa obowiązuje wszystkich pracowników Starostwa Powiatowego w Myśliborzu.

Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.

1. Administrator Danych Osobowych, którym jest Starosta Myśliborski, wyznacza Administratora Bezpieczeństwa Informacji (ABI), Z-cę Administratora Bezpieczeństwa Informacji oraz Lokalnych Administratorów Bezpieczeństwa Informacji (LABI).
2. Administrator Bezpieczeństwa Informacji oraz Lokalny Administrator Bezpieczeństwa Informacji (LABI) w swoich obszarach realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu oraz zbiorach tradycyjnych,
   2) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
   3) niezwłocznego informowania Administratora Danych Osobowych (Starosty) lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   4) nadzoru i kontroli zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
   5) monitorowania fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane.

3. W przypadku nieobecności Administratora Bezpieczeństwa Informacji powyższe *zadana* realizuje jego zastępca. Zastępca ze wszystkich podjętych działań składa Administratorowi Bezpieczeństwa Informacji relację w formie pisemnej notatki.

Polityka bezpieczeństwa danych osobowych została opracowana na podstawie następujących aktów prawnych:

1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, póz. 926 z późn. zm.),
2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Definicje

- Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- Administrator Danych Osobowych - zadania administratora danych osobowych wykonuje Starosta Myśliborski.
- Administrator Bezpieczeństwa Informacji - osoba wyznaczona przez Administratora Danych Osobowych nadzorującą całokształt zagadnień związanych z ochroną danych osobowych
- Lokalny Administrator Bezpieczeństwa Informacji – osoba wyznaczona przez Administratora Danych Osobowych nadzorująca zagadnienia związane z ochroną danych osobowych w podległej komórce organizacyjnej
- Administrator Systemu Informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych.
- System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
- Bezpieczeństwo systemu informatycznego - wdrożenie przez Administratora Danych Osobowych środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
- Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- Osoba upoważniona - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych na wniosek Administratora Bezpieczeństwa Informacji i dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu (ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji).
- Użytkownik systemu - osoba posiadająca uprawnienia umożliwiające dostęp do systemu informatycznego, w którym są przetwarzane dane osobowe.
- Ustawa - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
- Rozporządzenie - rozporządzenie 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.

Rozdział 1

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 pracy systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, obniżenie sprawności i wydajności sprzętu i oprogramowania związane z jego eksploatacją) - mogą prowadzić do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu lub nastąpić naruszenie poufności danych.
   3) Zagrożenia zamierzone - świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      - nieuprawniony dostęp do systemu z jego wnętrza (naruszenie zabezpieczeń),
      - nieuprawnione przekazanie danych,
      - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).
2. Naruszenie lub podejrzenie naruszenia zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:
   1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
   2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
   4) pojawienia się odpowiedniego komunikatu alarmowego,
   5) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
   6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
   7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
   8) ujawnienia nieautoryzowanych kont dostępu do systemu,
   9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).
4. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.
   - niezabezpieczone pomieszczenia ze szczególnym uwzględnieniem pomieszczenia serwerowni,
   - nienadzorowane, otwarte szafy, biurka, regały,
   - niezabezpieczone urządzenia i nośniki do archiwizacji,
   - pozostawianie danych w nieodpowiednich miejscach - biurka, półki na dokumenty itp.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem Danych Osobowych gromadzonych i przetwarzanych w sposób tradycyjny i w systemach informatycznych Urzędu jest Starosta Myśliborski (wykaz zbiorów danych osobowych przetwarzanych w Urzędzie wraz z nazwą systemu służącego do ich przetwarzania oraz ich strukturą i zakresem stanowi załącznik nr 1 do niniejszego dokumentu).
2. Tworzenie nowego bądź modyfikacja struktury lub zakresu danych istniejącego zbioru podlega obowiązkowi zgłoszenia Administratorowi Danych Osobowych za pośrednictwem Administratora Bezpieczeństwa Informacji. Obowiązek spoczywa na osobie tworzącej lub modyfikującej zbiór danych osobowych.
3. Przetwarzanie zbioru danych osobowych można rozpocząć po zgłoszeniu tego zbioru Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji a w przypadku zbiorów, o których mowa w art.27 ust.1 ustawy po ich rejestracji chyba, że ustawa zwalnia z tego obowiązku. Rejestracja odbywa się na podstawie zgłoszenia stanowiącego załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r.w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. nr 229 póz. 1536).
   Zgłoszenie dotyczące rejestracji lub modyfikacji zarejestrowanego zbioru danych osobowych przygotowuje osoba tworząca lub modyfikująca zbiór i przedkłada je Administratorowi Danych Osobowych po akceptacji przez Administratora Bezpieczeństwa Informacji.
4. Administrator Danych Osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych przetwarzanych w sposób tradycyjny oraz w systemach informatycznych Urzędu, a w szczególności:
   1) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiega przed pobraniem danych przez osobę nieuprawnioną,
   3) zapobiega zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
   4) zapewnia przetwarzanie danych zgodnie z obowiązującymi przepisami prawa.
5. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:
   1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach,
   2) zabezpieczenie pomieszczeń, o których mowa w pkt. 1, przed nieuprawnionym dostępem:
      - klucze do pomieszczeń, w których następuje przetwarzanie danych osobowych wydawane są tylko osobom upoważnionym do przetwarzania danych w tych pomieszczeniach,
      - pomieszczenia, w których odbywa się przetwarzanie danych osobowych znajdują się pod ścisłym nadzorem pracujących w nim osób upoważnionych do przetwarzania danych,
   3) zabezpieczenie dostępu do komputerów, na których jest prowadzone przetwarzanie danych przez wprowadzenie systemu logowania zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego, określonymi w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,
   4) systematyczne wykonywanie kopi bezpieczeństwa danych na nośnikach zewnętrznych przechowywanych w sejfach lub szafach metalowych,
   5) zastosowanie zasilaczy UPS do zasilania awaryjnego serwerów, urządzeń dostępowych,
   6) aktywowanie na wszystkich stacjach roboczych ochrony antywirusowej,
   7) stosowanie zapory ogniowej (firewall) na ruterach dostępowych zabezpieczającej sieci przed atakiem z zewnątrz i filtrującej dostęp do sieci WAN poprzez blokowanie niektórych usług,
   8) umieszczenie większości urządzeń znajdujących się w serwerowniach w szafach

serwerowych i sieciowych oraz wyposażanie pomieszczeń serwerowni w urządzenia zapewniające właściwą temperaturę i wilgotność,

6. Organizacyjne środki ochrony danych osobowych i ich przetwarzania obejmują:
   1) zapoznanie każdej osoby upoważnionej z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu,
   2) przeszkolenie użytkowników systemu w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczeniem pomieszczeń i budynków,
   3) szczególne zabezpieczenie pomieszczenia serwerowni, do którego dostęp posiadają jedynie osoby upoważnione na piśmie przez Administratora Danych Osobowych (Starostę), wzór upoważnienia stanowi załącznik nr 3 do niniejszego dokumentu,
   4) dopuszczenie do przetwarzania danych osobowych jedynie osób posiadających upoważnienie oraz prowadzenie ewidencji tych osób.
7. Do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych Osobowych w toku następującej procedury:
   1) Lokalny Administrator Bezpieczeństwa Informacji (LABI) kieruje do Administratora Bezpieczeństwa Informacji wniosek o wydanie upoważnienia do przetwarzania danych osobowych określając:
      - dane użytkownika
      - zbiór danych osobowych
      - zakres przetwarzanych danych osobowych,

      (wzór wniosku stanowi załącznik nr 4 do niniejszego dokumentu)
   2) Administrator Bezpieczeństwa Informacji przedkłada Administratorowi Danych Osobowych (Staroście) do akceptacji wniosek oraz upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik nr 5)
   3) po zaakceptowaniu przez Starostę wniosku i wystawieniu upoważnienia
      - Administrator Bezpieczeństwa Informacji/Lokalny Administrator Bezpieczeństwa Informacji zapoznaje nowego użytkownika z Polityką bezpieczeństwa, Instrukcją zarządzania systemami informatycznymi, Ustawą i Rozporządzeniem oraz wprowadza użytkownika do ewidencji osób zapoznanych z dokumentacją (wzór stanowi załącznik nr 8) oraz do ewidencji osób upoważnionych do przetwarzania danych osobowych (wzór stanowi załącznik nr 6),
      - zapoznanie się *z* powyższymi regulacjami pracownik potwierdza Administratorowi Bezpieczeństwa Informacji/ Lokalnemu Administratorowi Bezpieczeństwa Informacji własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 7 do niniejszego dokumentu
8. Modyfikacja lub odebranie pracownikowi upoważnienia do przetwarzania danych osobowych następuje na pisemny wniosek przełożonego pracownika i podlega analogicznej procedurze jak przy jego nadawaniu.
9. Przepływ danych pomiędzy systemami informatycznymi służącymi do przetwarzania danych osobowych odbywa się w poszczególnych budynkach Urzędu z wykorzystaniem wewnętrznej zamkniętej sieci LAN.
10. Wykaz obszarów, w których przetwarzane są dane osobowe stanowi załącznik nr 2 do niniejszego dokumentu.
11. Niezależnie od niniejszych ustaleń mają zastosowanie wszelkie inne regulaminy i instrukcje dotyczące bezpieczeństwa.

Rozdział 3
KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator Bezpieczeństwa Informacji oraz Lokalni Administratorzy Bezpieczeństwa Informacji sprawują w imieniu Administratora Danych Osobowych nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z ustawy o ochronie danych osobowych, zasad ustanowionych w niniejszym dokumencie oraz instrukcji zarządzana systemami informatycznymi.
2. Każdy pracownik Starostwa Powiatowego w Myśliborzu jest zobowiązany poddać się kontroli wynikającej z ochrony danych osobowych prowadzanej przez Administratora Bezpieczeństwa Informacji oraz udostępnić niezbędne informacje mające wpływ na bezpieczeństwo danych.
3. Na podstawie kontroli oraz zgłoszeń naruszenia bezpieczeństwa danych osobowych, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie, które przedstawia Staroście.

Rozdział 4
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) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

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

   każda osoba zatrudniona w Starostwie jest zobowiązana do niezwłocznego powiadomienia o fakcie naruszenia bezpieczeństwa ochrony danych osobowych bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji.

Po stwierdzeniu naruszenia opisanego w ust. 1 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 zdarzenia,
4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,

6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub jego zastępcy,
7) niezwłocznie po przybyciu Administratora Bezpieczeństwa Informacji wypełnić zgłoszenie naruszenia bezpieczeństwa danych osobowych (wzór zgłoszenia stanowi załącznik nr 9).

3. Po przybyciu na miejsce naruszenia lub ujawnienia danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowej pracy Urzędu,
   2) może zażądać dokładnej relacji na piśmie z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) w razie potrzeby powiadamia o zaistniałym naruszeniu Administratora Danych Osobowych,
   4) jeżeli zachodzi taka potrzeba zleca usuniecie występujących naruszeń Administratorowi Systemów Informatycznych oraz powiadamia odpowiednie instytucje.
4. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 10.
5. Raport, o którym mowa w ust. 4, Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych (Staroście).
6. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Starostę.
7. Analiza, o której mowa w pkt. 6, powinna zawierać wszechstronną ocenę zaistniałego naruszenia oraz wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5
ZASADY UDOSTĘPNIENIA DANYCH OSOBOWYCH.

1. Dane osobowe gromadzone i przetwarzane w Urzędzie mogą być udostępniane wyłącznie osobom uprawnionym na podstawie wniosku o udostępnienie danych osobowych (wzór wniosku stanowi załącznik nr 11 do niniejszego dokumentu) lub realizującym zadania ustawowe,
2. Bez względu na formę udostępniania danych należy zachować ich poufność i integralność. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani inną uniemożliwiającą ustalenie tożsamości osoby uzyskującej dostęp do danych.

Rozdziale 6
POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, 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.
3. W kwestiach nieuregulowanych w niniejszym dokumencie a dotyczących bezpieczeństwa danych osobowych w Starostwie Powiatowym w Myśliborzu decyzje na wniosek zainteresowanego wydaje Administrator Danych Osobowych (Starosta)

Załącznik nr 1
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

4. Wykaz zbiorów danych osobowych wraz z nazwą systemu służącego do ich przetwarzania oraz ich strukturą

Lp.	Nazwa zbioru (w postaci elektronicznej lub papierowej)	System informatyczny (dotyczy zbiorów w postaci elektronicznej)	Opis gromadzonych danych	
1	Zgłaszanie i przyjmowanie do zasobu prac geodezyjnych oraz uzgadnianie usytuowania projektowych sieci uzbrojenia terenu	GEO-INFO	Osoby fizyczne	Imię, Nazwisko, ulica i nr, kod pocztowy, miejscowość, PESEL, NIP
2	Ewidencja gruntów i budynków Starostwa Powiatowego w Myśliborzu	GEO-INFO	Osoby fizyczne	Imię, Nazwisko, ulica i nr, kod pocztowy, miejscowość, PESEL, NIP
3	Ewidencja zezwoleń na sprowadzenie zwłok lub szczątków ludzkich z zagranicy	Forma papierowa	Wnioskodawca	Nazwisko i imię, ulica i nr, kod pocztowy miejscowość, nr telefonu, seria i nr dokumentu tożsamości, nr telefonu, fax-u, NIP, data i nr decyzji
4	Ewidencja pracowników	R2Płatnik	pracownik	Nazwisko i mię, adres zamieszkania, PESEL, NIP, nr dowodu osobistego, data urodzenia, nazwisko panieńskie, wynagrodzenie, dodatek funkcyjny, dodatek stażowy, wymiar czasu pracy, okres zatrudnienia, nieobecności, urlopy wypoczynkowe, okolicznościowe, macierzyński, wychowawcze, bezpłatne), imiona rodziców, płeć, przebieg
5	ZUS pracowników	Płatnik	pracownik	Nazwisko, Imię, adres zamieszkania, PESEL, NIP, nr dowodu osobistego, data urodzenia, obywatelstwo, płeć, data założenia kartoteki, data powstania obowiązku ubezpieczenia, kod tytułu ubezpieczenia, oddział ZUS, przynależność do NFZ, rodzaj

6	Rejestr skarg i wniosków	Forma papierowa	Skarżący lub wnioskodawca	Data otrzymania; skąd otrzymano, nazwisko, imię, adres wnoszącego skargę lub wniosek; treść skargi lub wniosku; komu przekazano; data przekazania; data otrzymania wyjaśnień, sposób załatwienia; termin udzielenia odpowiedzi.
7	Rejestr skarg i wniosków rozpatrywanych przez Radę Powiatu	Forma papierowa	Skarżący lub wnioskodawca	Data otrzymania; skąd otrzymano, nazwisko, imię, adres wnoszącego skargę lub wniosek; treść skargi lub wniosku; komu przekazano; data przekazania; data otrzymania wyjaśnień, sposób załatwienia; termin udzielenia odpowiedzi.
8	Ewidencja rzeczy znalezionych	Forma papierowa	Znalazca	Data otrzymania zawiadomienia o znalezieniu *rzeczy;* imię, nazwisko oraz adres znalazcy; opis *rzeczy* znalezionej (rodzaj, ilość); miejsce przechowywania rzeczy; data wystania powiadomienia lub
9	Kontrahenci	Program finansowo - księgowy FOKA	Osoby fizyczne i prawne	Imię, nazwisko, adres
10	Kontrahenci	Ośrodek GEO-INFO	Osoby fizyczne i prawne	Imię, nazwisko, adres
11	Radni Rady Powiatu Myśliborskiego	Forma papierowa	radny	Imię, nazwisko, nr tel. służbowego, komórkowego, prywatnego, adres zamieszkania, adres e-mailowy
12	Oświadczenia majątkowe pracowników Starostwa Powiatowego i jednostek organizacyjnych	Forma papierowa	osoba	Imię, nazwisko, adres, data urodzenia, NIP, PESEL, dochody
13	Oświadczenia majątkowe radnych Rady Powiatu w Myśliborzu	Forma papierowa	osoba	Imię, nazwisko, adres, data urodzenia, NIP, PESEL, dochody
14	Elektroniczny Obieg Dokumentów	Program E-urząd	Osoby fizyczne i prawne	Imię, nazwisko, adres, NIP, PESEL,
15	Rejestr zwierząt podlegających ograniczeniom na podstawie umów międzynarodowych	Forma papierowa	Właściciel	imię, nazwisko, adres albo nazwę i siedzibę posiadacza lub prowadzącego hodowlę, adres miejsca przetrzymywania zwierząt lub prowadzenia hodowli, liczba zwierząt posiadanych lub hodowanych, nazwa gatunku w języku łacińskim i polskim,
16	Rejestr sprzętu pływającego służącego do połowu ryb posiadanego przez uprawnionego do rybactwa.	Forma papierowa	Właściciel	imię i nazwisko, miejsce zamieszkania i adres albo nazwa i adres posiadacza sprzętu, nadany dla sprzętu pływającego numer rejestracyjny,

17	Rejestr sprzętu pływającego służącego do amatorskiego połowu ryb.	Forma papierowa	Właściciel	imię i nazwisko, miejsce zamieszkania i adres albo nazwa i adres posiadacza sprzętu, nadany dla sprzętu pływającego numer rejestracyjny,
18	Rejestr wydawanych kart wędkarskich i kart łowiectwa podwodnego	Forma papierowa		imię i nazwisko, adres, data urodzenia, miejsce urodzenia, PESEL, seria i numer dowodu osobistego
19	Rejestr wniosków o pozwolenie na budowę	Forma papierowa	Inwestor	imię i nazwisko/ nazwa firmy, ulica i numer, kod pocztowy, miejscowość, numer działki, numer decyzji
20	Rejestr decyzji o pozwoleniu na budowę	Forma papierowa	Inwestor	imię i nazwisko, ulica i numer, kod pocztowy, miejscowość, numer działki, numer decyzji
21	Ewidencja wniosków o wydanie licencji na krajowy transport drogowy rzeczy lub osób	Licencje, zezwolenia zaświadczenia na przewóz osób i rzeczy firmy INFORMICA Milanówek	kierowca	nazwiska, imiona, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, numer telefonu
22	Ewidencja pojazdów	POJAZD firmy PROKOM	właściciel pojazdu	nazwiska, imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, seria i numer dowodu
23	Ewidencja kierowców	MOUN firmy PROKOM	kierowca lub osoba bez uprawnień	nazwiska, imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer telefonu, wizerunek (zdjęcie), numery identyfikacyjne (numer w rejestrze, numer karty kierowcy), świadectwa kwalifikacji, informacje dot. prawa jazdy i kwalifikacji (numer prawa jazdy, ważność, data uzyskania, ograniczenia, kategorie), orzeczenie lekarskie stwierdzające brak
24	Podania o wpis do ewidencji instruktorów Starostwa Powiatowego w Myśliborzu	Forma papierowa	instruktor	nazwiska, imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, numer telefonu, zakres uprawnień, stan zdrowia
25	Dokumentacja stacji kontroli pojazdów Starostwa Powiatowego w Myśliborzu	Forma papierowa	instruktor	nazwiska, imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, numer telefonu, zakres uprawnień, stan zdrowia

26	Ewidencja wydanych i cofniętych uprawnień diagnostom	Forma papierowa	diagnosta	nazwiska, imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, numer telefonu, dane potwierdzające praktykę zawodową, dane dot. wymaganych szkoleń i egzaminu kwalifikacyjnego
27	Ewidencja wydanych kart parkingowych	Forma papierowa	osoba niepełnosprawna	nazwiska, imiona, adres zamieszkania lub pobytu, data ważności orzeczenia o stopniu niepełnosprawności, stopień niepełnosprawności
28	Nauczyciele, wychowawcy i inni pracownicy pedagogiczni szkół i placówek prowadzonych przez Radę Powiatu w Myśliborzu	SIO-System Informacji Oświatowej	nauczyciel	PESEL - zakodowany, płeć, rok urodzenia, stopień awansu zawodowego, wykształcenie, podstawa prawna świadczenia pracy, miejsce nawiązania stosunku pracy, tyg. wymiar zajęć, godz. ponadwymiarowe, zwiększony wymiar zajęć, ogólny staż pracy, staż pracy pedagogicznej, stanowisko/funkcja, wynagrodzenie, zasadnicze, dodatek za wysługę lat, dod. funkcyjny wynikający z pełnienia funkcji kierowniczej, dodatek z tytułu pełnienia funkcji opiekuna stażu, dodatek za wychowawstwo klasy, za pełnienie funkcji nauczyciela doradcy, dodatek za warunki pracy,

Załącznik nr 2
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

Wykaz obszarów, w których przetwarzane są dane osobowe

Lp.	**Nazwa zbioru danych osobowych** (w postaci elektronicznej lub papierowej)	**Lokalizacja** (adres, komórka organizacyjna, kondygnacja, nr pokoju)
1	Zgłaszanie i przyjmowanie do zasobu prac geodezyjnych oraz uzgadnianie usytuowania projektowych sieci	budynek przy ul. Spokojnej 13 w Myśliborzu Wydział Geodezji Katastru i Gospodarki Nieruchomościami
2	Ewidencja gruntów i budynków Starostwa Powiatowego w Myśliborzu	budynek przy ul. Spokojnej 13 w Myśliborzu Wydział Geodezji Katastru i Gospodarki Nieruchomościami
3	Ewidencja zezwoleń na sprowadzenie zwłok lub szczątków ludzkich z zagranicy	budynek przy ul. Północnej 15 w Myśliborzu , Wydział Edukacji, Zdrowia i Spraw Społecznych
4	Ewidencja pracowników	budynek przy ul. Spokojnej 22 w Myśliborzu, Wydział Organizacyjno – Prawny
5	ZUS pracowników	budynek przy ul. Spokojnej 22 w Myśliborzu, Wydział Finansowy
6	Rejestr skarg i wniosków	budynek przy ul. Spokojnej 22 w Myśliborzu, Wydział Organizacyjno – Prawny
7	Rejestr skarg i wniosków rozpatrywanych przez radę powiatu	budynek przy ul. Spokojnej 22 w Myśliborzu, Biuro Obsługi Rady i Zarządu
8	Ewidencja rzeczy	budynek przy ul. Spokojnej 22 w Myśliborzu, Wydział Organizacyjno – Prawny
9	Kontrahenci FOKA	budynek przy ul. Spokojnej 22 w Myśliborzu, Wydział Finansowy
10	Kontrahenci GEO-INFO	budynek przy ul. Spokojnej 13 w Myśliborzu Wydział Geodezji Katastru i Gospodarki Nieruchomościami
11	Radni Rady Powiatu Myśliborskiego	budynek przy ul. Spokojna 22 , Biuro Obsługi Rady i Zarządu
12	Oświadczenia majątkowe pracowników Starostwa Powiatowego i jednostek organizacyjnych	budynek przy ul. Spokojnej 22 w Myśliborzu, Wydział Organizacyjno – Prawny, Biuro Obsługi Rady i Zarządu
13	Oświadczenia majątkowe radnych rady powiatu	budynek przy ul. Spokojna 22 , Biuro Obsługi Rady i Zarządu
14	Elektroniczny Obieg Dokumentów	budynek przy ul. Spokojnej 22 w Myśliborzu, Wydział Organizacyjno – Prawny, Biuro Obsługi Rady i Zarządu
15	Rejestr zwierząt podlegających ograniczeniom na podstawie umów międzynarodowych	Budynek przy ul. Spokojnej 13, Wydział Budownictwa i Ochrony Środowiska
16	Rejestr sprzętu pływającego służącego do połowu ryb posiadanego przez uprawnionego do rybactwa.	Budynek przy ul. Spokojnej 13, Wydział Budownictwa i Ochrony Środowiska

17	Rejestr sprzętu pływającego służącego do amatorskiego połowu ryb.	Budynek przy ul. Spokojnej 13, Wydział Budownictwa i Ochrony Środowiska
18	Rejestr wydawanych kart wędkarskich i kart łowiectwa podwodnego	Budynek przy ul. Spokojnej 13, Wydział Budownictwa i Ochrony Środowiska
19	Rejestr wniosków o pozwolenie na budowę	Budynek przy ul. Spokojnej 13, Wydział Budownictwa i Ochrony Środowiska
20	Rejestr decyzji o pozwoleniu na budowę	Budynek przy ul. Spokojnej 13, Wydział Budownictwa i Ochrony Środowiska
21	Ewidencja wniosków o wydanie licencji na krajowy transport drogowy rzeczy lub osób	Budynek przy ul. Północnej 15, Wydział Komunikacji
22	Ewidencja pojazdów	Budynek przy ul. Północnej 15, Wydział Komunikacji
23	Ewidencja kierowców	Budynek przy ul. Północnej 15, Wydział Komunikacji
24	Podania o wpis do ewidencji instruktorów Starostwa Powiatowego w Myśliborzu	Budynek przy ul. Północnej 15, Wydział Komunikacji
25	Dokumentacja stacji kontroli pojazdów Starostwa Powiatowego w Myśliborzu	Budynek przy ul. Północnej 15, Wydział Komunikacji
26	Ewidencja wydanych i cofniętych uprawnień diagnostom	Budynek przy ul. Północnej 15, Wydział Komunikacji
27	Ewidencja wydanych kart parkingowych	budynek przy ul. Północnej 15 w Myśliborzu , Zespół ds. Orzekania o Niepełnosprawności
28	Nauczyciele, wychowawcy i inni pracownicy pedagogiczni szkół i placówek prowadzonych przez Radę	Budynek przy ul. Spokojna 22, Wydział Edukacji, Zdrowia i Spraw Społecznych

Załącznik nr 3
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

UPOWAŻNIENIE NR .....

Upoważniam Panią/Pana .....

(imię i nazwisko)

pracownika wydziału .....

(jednostka organizacyjna)

do pobierania kluczy i dostępu do pomieszczenia serwerowni znajdującego się w

.....

(lokalizacja pomieszczenia)

UZASADNIENIE DOSTĘPU

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

Upoważnienie ważne* bezterminowo/do dnia .....

....

(data) (podpis Starosty Myśliborskiego)

*niepotrzebne skreślić

Załącznik nr 4
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

WNIOSEK
O WYDANIE/ODEBRANIE UPOWAŻNIENIA
DO PRZETWARZANIA DANYCH OSOBOWYCH

.....
nazwa zbioru danych osobowych/systemu informatycznego

☐ Nowe upoważnienie	☐ Modyfikacja upoważnienia	☐ Odebranie upoważnienia

imię i nazwisko pracownika	**Jednostka organizacyjna/stanowisko**
Zakres upoważnienia do przetwarzania danych osobowych	
Data:	Podpis bezpośredniego przełożonego użytkownika systemu

Podpis Administratora Bezpieczeństwa Informacji	AKCEPTACJA Administratora Danych Osobowych (Starosta)

Załącznik nr 5
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

UPOWAŻNIENIE NR .....

Upoważniam Panią/Pana .....

(imię i nazwisko)

pracownika wydziału .....

(jednostka organizacyjna)

do przetwarzania danych osobowych w zbiorze

.....

(nazwa zbioru danych osobowych/systemu informatycznego)

w zakresie:

.....

(uzasadnienie dostępu)

.....

.....

.....

Upoważnienie ważne* bezterminowo/do dnia .....

Zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) osoby, które zostały upoważnione do przetwarzania danych są obowiązane zachować w tajemnicy przetwarzanie dane osobowe oraz sposoby ich zabezpieczenia.

....

(data) (podpis Starosty Myśliborskiego)

*niepotrzebne skreślić

Załącznik nr 6

do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

EW IDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Zbiór danych osobowych/System	Nazwisko i imię/ Identyfikator w systemie	Numer upoważnienia	Data wydania (modyfikacji) upoważnienia	Data utraty ważności upoważnienia	Zakres upoważnienia do przetwarzania danych osobowych	Podpis ABI

Załącznik nr 7
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

Myślibórz, dnia.....

.....
(nazwisko i imię)

.....
(nazwa komórki/ stanowisko)

.....
(numer upoważnienia)

OŚWIADCZENIE

Oświadczam, iż w związku z przetwarzaniem danych osobowych wynikających z wykonywanych przeze mnie czynności służbowych zapoznałem(am) się z:

1. Ustawą z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. Nr 133, póz. 883 z poźn. zm.),
2. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, póz. 1024).
3. Dokumentem „Polityka bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Myśliborzu".
4. Dokumentem „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Myśliborzu".

.....
(podpis pracownika)

Załącznik nr 8
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

Ewidencja osób,

które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych" służących do przetwarzania danych osobowych w Starostwie Powiatowym w Myśliborzu., Instrukcją zarządzania systemami informatycznymi, zapisami zawartymi w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997r. oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa i Instrukcji zarządzania systemami informatycznymi.

Lp.	Nazwisko i imię	Komórka organizacyjna	Data, podpis

Załącznik nr 9
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

Z G Ł O S Z E N I E

naruszenia bezpieczeństwa danych osobowych w Starostwie Powiatowym w Myśliborzu

1. Data:……Godzina:.....
   (dd.mm.mr) *(00:00)*
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   .....
   (imię i nazwisko, stanowisko służbowe)
3. Lokalizacja zdarzenia:

   .....
   (nr pokoju, nazwa pomieszczenia, stanowisko pracy, system informatyczny)
4. Opis zaistniałej sytuacji wpływającej na bezpieczeństwo danych osobowych:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

☐ : ☐ ☐

....

godz. i data przyjęcia podpis osoby zgłaszającej

podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 10
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

Raport ze zgłoszenia
naruszenia bezpieczeństwa danych osobowych
w Starostwie Powiatowym w Myśliborzu

1. Data:..... .....Godzina:.....

(dd.mm.mr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię i nazwisko, stanowisko służbowe)

3.Lokalizacja zdarzenia:

.....

(nr pokoju, nazwa pomieszczenia, stanowisko pracy, system informatyczny)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

5. Podjęte działania:

.....

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

.....

podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 11
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w Starostwie Powiatowym w Myśliborzu

WNIOSEK
O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do Starosty Myśliborskiego

2. Wnioskodawca.....
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych osobowych:
.....
.....
.....* ☐ ew.cd. w załączniku nr

4. Wskazanie przeznaczenia dla udostępnionych danych:
.....
.....* ☐ ew.cd. w załączniku nr

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:
.....
.....

6.Zakres żądanych informacji ze zbioru:
.....
.....* ☐ ew.cd. w załączniku nr

7.Informacje umożliwiające wyszukanie w zbiorze żądanych danych:
.....
.....* ☐ ew.cd. w załączniku nr

.....
* Jeżeli TAK, to zakreśl kwadrat literą „x":
(miejsce na znaczki opłaty skarbowej)

.....
(data, podpis i ewentualnie pieczęć wnioskodawcy)