

**Załącznik Nr 1
do zarządzenia B M i G
Nr 0050. 39. 2011
z dnia 17 maja 2011 roku**

**Polityka bezpieczeństwa i instrukcja zarządzania systemem
informatycznym służącym do przetwarzania danych osobowych**

w Urzędzie Miasta i Gminy Małogoszcz

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 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), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

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) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- 7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- 8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
- 9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy 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) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
- 12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- 13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie 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

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Miasta i Gminy Małogoszcz jest Burmistrz.

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 przed zabraniem 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) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
- 4) 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,
- 1) 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.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa w Urzędzie Miasta i Gminy Małogoszcz” w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Urzędu Miasta i Gminy Małogoszcz i ich zabezpieczeń zawiera załącznik **nr 1** do niniejszego dokumentu.

7. Opis struktur zbiorów danych osobowych prowadzonych w Urzędzie Miasta i Gminy Małogoszcz zawiera załącznik **nr 2** do niniejszego dokumentu

8. W celu ochrony przed utratą danych w Urzędzie Miasta i Gminy Małogoszcz stosowane są następujące zabezpieczenia:

- 1) *odrębne zasilanie sprzętu komputerowego,*
- 2) *ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,*
- 3) *ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na taśmach magnetycznych, nośnikach DVD z których w przypadku awarii odtwarzane są dane i system operacyjny*
- 4) *ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.*

Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu (zastosowanie elementów hotswap i hotspare).

Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

- 1) *wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji.*
- 2) *aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.*
- 3) *w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie logowania się do system operacyjnego 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.*

Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez internet.

W zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniami, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry.

Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.

Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

- 1) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,*
- 2) filtrowanie pakietów i blokowanie niektórych usług,*
- 3) objęcie ochroną antywirusową wszystkich danych ściąganych z internetu na stacjach lokalnych,*
- 4) zapisywanie logów połączeń użytkowników z siecią Internet*

Postanowienia końcowe.

- 1) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami.*
- 2) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.*
- 3) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytych szkoleniach z zakresu ustawy o ochronie danych osobowych.*
- 4) w pomieszczeniach w których znajdują się serwery zamontowane są czujniki dymu.*
- 5) w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego*
- 6) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.*
- 7) większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.*

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji” sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa sporządza półroczne plany kontroli zatwierdzone przez Burmistrza i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych (Burmistrzowi).

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) 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. zalenie, pożar, itp.)

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego,

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, 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 Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

- 1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości

- pracy Urzędu,
- 2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
 - 3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora danych ,
 - 4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **nr 3**, który powinien zawierać w szczególności:

- 1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- 2) określenie czasu i miejsca naruszenia i powiadomienia,
- 3) określenie okoliczności towarzyszących i rodzaju naruszenia,
- 4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- 5) wstępną ocenę przyczyn wystąpienia naruszenia,
- 6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 6, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych (Burmistrzowi), a w przypadku jego nieobecności osobie uprawnionej.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

9. Analiza, o której mowa w ust. 9, 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 5

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) kontrola ewidencji nośników magnetycznych,
 - c) kontrola właściwej częstotliwości zmiany hasła .

Rozdział 6

SZKOLENIA

1. Wszyscy pracownicy Urzędu mają obowiązek brać udział w szkoleniach ,
2. Szkolenie powinno dotyczyć:
 - a) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
 - b) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział 7

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.,
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika,
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji,
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 8

ARCHIWIZACJA DANYCH

1. Dane systemów kopiowane są w systemie tygodniowym,
2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie,
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji,
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w (kasa Urzędu, kancelaria tajna itp.),
5. Kopie awaryjne przechowywane są w (*kasa pancerna, szafa metalowa - w wyznaczonym pomieszczeniu lub instytucji , z którą podpisano stosowne porozumienie*),
6. Dyskietki , na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane , w taki sposób , by nie można było odtworzyć ich zawartości.
7. Płyty CD , DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny , tak by nie można było użyć ich ponownie,

8. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne,
9. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności.

Rozdział 9

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 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 4** 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.

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 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), 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 rozporządzenie 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).

6. *Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Małogoszcz” wchodzi w życie z dniem jej podpisania przez Burmistrza.*

Załącznik nr 1 do „Polityki bezpieczeństwa”

Miejsmem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych Urzędu Miasta i Gminy Małogoszcz mieszczące się na parterze i I piętrze budynku Urzędu w miejscowości Małogoszcz ul. Jaszowskiego 3A

Granice obszarów oraz osoby i referaty (samodzielne stanowiska pracy), które przetwarzają dane osobowe.

POKÓJ NR 2 – parter- OBSŁUGA Dodatków Mieszkaniowych oraz programów Fundusz alimentacyjny, Świadczenia rodzinne	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Chabior Małgorzata - Machnik Wioletta

POKÓJ NR 3 – parter- OBSŁUGA programów Kadry, Urząd Stanu Cywilnego	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Modzelewska Dorota - Gogół Mieczysława

POKÓJ NR 4 – parter - OBSŁUGA programu Dowody osobiste	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Bogucka Barbara - Kucharska Maria

POKÓJ NR 6 – parter - OBSŁUGA programów Ewidencja ludności, Wyborcy	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Kucharska Maria - Bogucka Barbara

POKÓJ NR 9 – parter – OBSŁUGA Referatu Finansowego oraz programu Kasa	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Wiater Jagoda - Kraus Agnieszka

POKÓJ NR 15 – I piętro - OBSŁUGA stanowiska ds. gospodarki komunalnej	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Piasecki Krzysztof - Beltowska Małgorzata

POKÓJ NR 16 – I piętro - OBSŁUGA Referatu Finansowego oraz programów Windykacja	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Jopek Krystyna - Gogół Mieczysława

POKÓJ NR 16 – I piętro - OBSŁUGA stanowiska zastępcy kierownika USC oraz programów Ewidencja podmiotów EPG, Koncesje alkoholowe	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Gogół Mieczysława - Jopek Krystyna

POKÓJ NR 17 – I piętro - OBSŁUGA Referatu Finansowego oraz programów Podatki-os.fizyczne, Paliwa, OPJ, POST, Zaświadczenia, Kontrahenci.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Łabędzka Stanisława - Kraus Agnieszka - Rak Katarzyna

POKÓJ NR 19 – I piętro- OBSŁUGA Referatu Finansowego oraz programów Faktury, FK (finansowo – księgowy)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Szymkiewicz Iwona - Czerwiński Grzegorz

POKÓJ NR 19 – I piętro- OBSŁUGA Referatu Finansowego oraz programów Place – Saturn HR, Płatnik	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Kot Maria - Domińska Mirosława

POKÓJ NR 20 – I piętro- OBSŁUGA stanowiska ds. oświaty	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Niechciał Mariola

POKÓJ NR 21 – I piętro- OBSŁUGA Straży miejskiej	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Jaros Adam - Bazylewicz Adam

POKÓJ NR 24 – I piętro- OBSŁUGA stanowiska ds. gospodarki nieruchomościami i zarządu mieniem	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Beltowska Małgorzata - Piasecki Krzysztof

POKÓJ NR 25 – I piętro- OBSŁUGA stanowiska ds. organizacyjnych obsługi Rady i komisji	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Sobota Halina

POKÓJ NR 27 – I piętro- OBSŁUGA Referatu Budownictwa i Inwestycji	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Spurek Przemysław - Mendelska Justyna

POKÓJ NR 29 – I piętro- OBSŁUGA Referatu Budownictwa i Inwestycji	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> -Gołębiowski Andrzej - Machnik Mirosław

POKÓJ NR 30 – I piętro- OBSŁUGA Referatu Budownictwa i Inwestycji	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	<u>Imię i nazwisko:</u> - Machnik Mirosław - Juzoń Paweł

Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	
Administrator Danych	<u>Imię i nazwisko:</u> - Jan Głogowski
Sekretarz Gminy	<u>Imię i nazwisko:</u> - Elżbieta Rachuba
Administrator Bezpieczeństwa Informacji	<u>Imię i nazwisko:</u> - Bartosz Barański
Radca Prawny	<u>Imię i nazwisko:</u> -Wiesław Zagala
Audytór Wewnętrzny	<u>Imię i nazwisko:</u> - Sylwia Lolo

Załącznik nr 2 do „ Polityki bezpieczeństwa” - Opis struktur zbiorów danych.

Zbiór danych ŚWIADCZENIA RODZINNE zawiera następujące pola:

Dane osobowe
- imię i nazwisko
- data urodzenia
- numer NIP
- numer PESEL
- stan cywilny
- numer i seria dowodu osobistego
- obywatelstwo
- nazwa banku i numer konta
- numer telefonu
Dane adresowe
- adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu, kod)

Zbiór danych DODATKI MIESZKANIOWE zawiera następujące pola:

Dane osobowe
- imię i nazwisko
- data urodzenia
- miejsce pracy
- numer i seria dowodu osobistego
Dane adresowe
- adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu, kod)

Zbiór danych FUNDUSZ ALIMENTACYJNY zawiera następujące pola:

Dane osobowe
- imię i nazwisko
- imiona rodziców
- data urodzenia
- miejsce urodzenia
- numer PESEL
- numer NIP
- stan cywilny
- płeć
- obywatelstwo
- wykształcenie
- zawód
- miejsce pracy
- nazwa banku i numer konta
- numer i seria dowodu osobistego
Dane adresowe
- adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu, kod)

Zbiór danych AKTA STANU CYWILNEGO zawiera następujące pola:

- imiona i nazwiska
- imiona i nazwiska rodowe rodziców
- nazwisko rodowe, nazwisko z poprzedniego małżeństwa
- data urodzenia, data zawarcia małżeństwa, data zgonu
- miejsce urodzenia (miejscowość, państwo)
- numer PESEL
- stan cywilny
- imię (imiona) i nazwisko małżonka
- płeć
- wyznanie
- adres zamieszkania.
- kod pocztowy
- dokument tożsamości (seria, nr, nazwa i siedziba wystawcy)
- podpis osoby
- USC i nr aktu urodzenia, małżeństwa, zgonu
- adnotacje o uznaniu dziecka, separacji, rozwodzie
- obywatelstwo
- wykształcenie
- źródło dochodu (zatrudnienie, na utrzymaniu, bezrobocie)

Zbiór danych ZMIANA IMIENIA I NAZWISKA zawiera następujące pola:

- imię (imiona) i nazwisko
- nazwisko rodowe
- data urodzenia
- miejsce urodzenia (miejscowość)
- numer PESEL
- stan cywilny
- obywatelstwo
- adres zamieszkania.(miejscowość, ulica, nr domu, nr lokalu, kod pocztowy)
- dokument tożsamości (seria, nr, nazwa i siedziba wystawcy)
- podpis osoby
- USC i nr aktu urodzenia, małżeństwa
- imię (imiona) i nazwisko nieletnich dzieci
- USC i nr aktu urodzenia nieletnich dzieci

Zbiór danych DOWODY OSOBISTE zawiera następujące pola:

- imiona i nazwiska,
- imiona i nazwiska rodowe rodziców
- nazwisko rodowe
- data urodzenia
- miejsce urodzenia
- numer PESEL
- kolor oczu
- wzrost w cm
- płeć
- adres zamieszkania.
- rodzaj zameldowania
- kod pocztowy

- posiadany dotychczasowy dokument tożsamości (seria, nr, nazwa i siedziba wystawcy)
- przyczyna wystawienia dowodu
- data i przyczyna utraty
- podpis osoby
- fotografia
- rejestry dowodów osobistych wydanych przed 31.12.2000 r.
- archiwum dowodów osobistych wydanych stałym mieszkańcom gminy
- archiwum dowodów osobistych wydanych i unieważnionych dla osób zmarłych

Zbiór danych EWIDENCJA LUDNOŚCI zawiera następujące pola:

Dane osobowe
- nazwiska i imię (imiona)
- nazwisko rodowe
- imiona i nazwiska rodowe rodziców
- data urodzenia
- miejsce urodzenia
- kraj urodzenia
- stan cywilny
- nr aktu urodzenia i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony
- płeć
- numer PESEL
- obywatelstwo albo status bezpaństwowca
- imię i nazwisko rodowe oraz numer PESEL małżonka, jeżeli został mu nadany
- data zawarcia związku małżeńskiego , numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego , w którym ten akt został sporządzony , data rozwiązania związku małżeńskiego , sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt i oznaczenie sądu , który ustalił nieistnienie małżeństwa, sygnatura akt i oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, numer jego aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony
- adres i data zameldowania na pobyt stały
- kraj miejsca zamieszkania
- data wymeldowania z miejsca pobytu stałego
- adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu
- data wymeldowania z miejsca pobytu czasowego
- data wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy i wskazanie kraju wyjazdu
- data powrotu z wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy
- seria, numer i data ważności ostatniego wydanego dowodu osobistego obywatela polskiego oraz oznaczenie organu wydającego dokument
- seria, numer i data ważności dokumentu podróży cudzoziemca, a w przypadku cudzoziemców ważnego dokumentu podróży lub innego ważnego dokumentu potwierdzającego tożsamość i obywatelstwo
- data upływu deklarowanego przez cudzoziemca terminu pobytu
- data zgonu albo data znalezienia zwłok, nr aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony.
Dane osobowe archiwalne
- nazwiska i imiona poprzednie

- nazwisko rodowe i z poprzedniego małżeństwa.
- kraj poprzedniego miejsca zamieszkania
Archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania
Archiwalne adresy czasowe oraz okresy pobytów czasowych
Poprzednio wydane dokumenty tożsamości
- rodzaj dokumentu
- seria i numer dowodu
- wystawca dokumentu
Stan cywilny archiwalny
- imię i nazwisko małżonka
- nazwisko rodowe i nazwisko z poprzedniego małżeństwa
- data zawarcia małżeństwa
- USC i numer aktu małżeństwa
Obowiązek wojskowy
- czy podlega obowiązkowi
- nazwa i nr wojskowego dokumentu tożsamości
- stopień wojskowy
Obywatelstwo (data zmiany, podstawa prawna)

Zbiór danych ZEZWOLENIA NA USUNIĘCIE DRZEW I KRZEWÓW
zawiera następujące pola:

Nazwisko i imię
Adres zamieszkania
Numery działek
Miejsce położenia działek
Numery dokumentów własności

Zbiór danych DZIAŁALNOŚĆ KOMISJI DO SPRAW ROZWIĄZYWANIA
PROBLEMÓW ALKOHOLOWYCH zawiera następujące pola:

Dane osobowe
- imię i nazwisko
- imiona rodziców
- nazwisko rodowe
- data i miejsce urodzenia
- numer PESEL
- obywatelstwo
- stan cywilny i stan rodzinny
- imię i nazwisko współmałżonka
- imię i nazwisko dzieci
- źródła utrzymania
- miejsce pracy
- wykształcenie
- zawód
- karalność
- podpis osoby
Dane adresowe
- adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu, kod)
- adres zameldowania

Zbiór danych REJESTR SKARG I WNIOSKÓW zawiera następujące pola:

- imiona i nazwiska
- adres zamieszkania

Zbiór danych REJESTR WYDANYCH ZEZWOLEŃ NA POSIADANIE PSÓW RAS UZNAWANYCH ZA AGRESYWNE zawiera następujące pola:

- imiona i nazwiska
- adres zamieszkania
- seria i numer dowodu osobistego

Zbiór danych REJESTR NAJEMCÓW KOMUNALNYCH I SOCJALNYCH LOKALI MIESZKALNYCH zawiera następujące pola:

- imiona i nazwiska
- adres zamieszkania
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego

Zbiór danych REJESTR WNIOSKÓW O PRZYDZIAŁ I ZMIANĘ LOKALI MIESZKALNYCH zawiera następujące pola:

- imiona i nazwiska
- adres zamieszkania
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego

Zbiór danych REJESTR ZEZWOLEŃ NA UPRAWĘ MAKU zawiera następujące pola:

- imię i nazwisko
- adres zamieszkania
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego

Zbiór danych EWIDENCJA OSÓB POSIADAJĄCYCH ZBIORNIKI BEZODPŁYWOWE zawiera następujące pola:

- imiona i nazwiska
- adres zamieszkania
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego

Zbiór danych EWIDENCJA OSÓB POSIADAJĄCYCH UMOWY ZAWARTE NA ODBIERANIE ODPADÓW KOMUNALNYCH zawiera następujące pola:

- imiona i nazwiska
- adres zamieszkania
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego

Zbiór danych REJESTR OSÓB SKŁADAJĄCYCH WNIOSKI O UDZIELENIE DOFINANSOWANIA NA USUWANIE AZBESTU zawiera następujące pola:

- imiona i nazwiska
- adres zamieszkania
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego
- numer NIP

Zbiór danych REJESTR POSTĘPOWANIA EGZEKUCYJNEGO zawiera następujące pola:

Dane osobowe
- nazwisko i imię
- imiona rodziców
- data urodzenia
- numer NIP
- numer PESEL
- adres zamieszkania lub pobytu
- miejsce pracy

Zbiór danych ZAROBKOWE WYKONYWANIE TRANSPORTU DROGOWEGO OSÓB zawiera następujące pola:

Dane osobowe
- nazwisko i imię
- adres zamieszkania lub pobytu
- numer ewidencyjny PESEL
- Numer Identyfikacji Podatkowej
- wykształcenie

Zbiór danych PODATKI zawiera następujące pola:

- imię i nazwisko
- data urodzenia
- imiona rodziców
- numer PESEL
- numer NIP
- adres zamieszkania
- numer telefonu
- numery aktów notarialnych
- numery ksiąg wieczystych
- numery działek

Zbiór danych ZWROT PODATKU AKCYZOWEGO zawiera następujące pola:

- imiona i nazwisko
- numer PESEL
- numer NIP
- numer i seria dowodu osobistego
- nazwa banku i numer konta
- adres zamieszkania

Zbiór danych STYPENDIA SOCJALNE zawiera następujące pola:

- imię i nazwisko wnioskodawcy
- data urodzenia
- imiona rodziców
- numer PESEL
- adres zamieszkania
- numer telefonu
- miejsce pracy
- informacja o dochodach

Zbiór danych MIANOWANIE NAUCZYCIELI zawiera następujące pola:

- imię i nazwisko wnioskodawcy
- data urodzenia
-adres zamieszkania
- numer telefonu
- miejsce pracy
- wykształcenie

Zbiór danych ARKUSZE ORGANIZACYJNE zawiera następujące pola:

- imię i nazwisko
- miejsce pracy
- wykształcenie

Zbiór danych SYSTEM INFORMACJI OŚWIATOWEJ zawiera następujące pola:

- rok urodzenia
- płeć
- numer PESEL
- wynagrodzenie
- forma zatrudnienia
- stopień awansu zawodowego
- wykształcenie
- stanowisko

**Zbiór danych REJESTR NAŁOŻONYCH MANDATÓW KARNYCH
zawiera następujące pola:**

- imię i nazwisko
- imiona rodziców
- data urodzenia
- miejsce urodzenia
- miejsce zamieszkania lub pobytu
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego

**Zbiór danych REJESTR NUMERACJI PORZĄDKOWEJ NIERUCHOMOŚCI
zawiera następujące pola:**

- imiona i nazwiska
- adres zamieszkania
- numery działek

**Zbiór danych REJESTR UŻYTKOWNIKÓW WIECZYSTYCH
zawiera następujące pola:**

- imiona i nazwiska
- adres zamieszkania
- numery działek
- numery aktów notarialnych

**Zbiór danych REJESTR DZIERŻAWCÓW I NAJEMCÓW
zawiera następujące pola:**

- imiona i nazwiska
- adres zamieszkania
- numery działek

**Zbiór danych EWIDENCJA OSÓB, KTÓRE WYKUPIŁY LOKALE MIESZKALNE
zawiera następujące pola:**

- imiona i nazwiska
- adres zamieszkania
- numer ewidencyjny PESEL
- seria i numer dowodu osobistego
- numer działek
- numery aktów notarialnych

**Zbiór danych OŚWIADCZENIA O STANIE MAJĄTKOWYM OSÓB
ZOBOWIĄZANYCH DO SKŁADANIA OŚWIADCZEŃ MAJĄTKOWYCH zawiera
następujące pola:**

- imię i nazwisko
- nazwisko rodowe
- data urodzenia
- miejsce urodzenia
- adres zamieszkania osoby składającej oświadczenie
- miejsce położenia nieruchomości (nr działek)

Zbiór danych KANDYDACI NA ŁAWNIKÓW zawiera następujące pola:

- imię i nazwisko
- nazwisko poprzednio używane
- imiona rodziców
- data i miejsce urodzenia
- obywatelstwo
- numer ewidencyjny PESEL
- numer NIP

- miejsce zamieszkania ze wskazaniem od ilu lat kandydat mieszka na terenie gminy
- adres do korespondencji i dane kontaktowe (numer telefonu domowego, numer telefonu w miejscu pracy i ewentualne adres e-mail)
- wykształcenie i kierunek(np. wykształcenie ekonomiczne, średnie zawodowe-technik budowlany)

Zbiór danych REJESTR DECYZJI USTALAJĄCYCH WARUNKI ZABUDOWY I ZAGOSPODAROWANIA zawiera następujące pola:

- nazwiska i imiona
- adres zamieszkania lub pobytu

Zbiór danych EWIDENCJA DECYZJI USTALAJĄCYCH JEDNORAZOWĄ OPŁATĘ Z TYTUŁU WARTOŚCI ZBYWANEJ NIERUCHOMOŚCI W ZWIĄZKU Z UCHWAŁANIEM PLANU MIEJSCOWEGO LUB JEGO ZMIANĄ zawiera następujące pola:

- nazwiska i imiona
- adres zamieszkania lub pobytu
- nr działek

Zbiór danych EWIDENCJA DECYZJI NA ZAJĘCIE PASA DROGOWEGO zawiera następujące pola:

- nazwiska i imiona
- adres zamieszkania lub pobytu
- nr działek

Załącznik nr 3 do „Polityki bezpieczeństwa „

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego w
Urzędzie Miasta i Gminy Małogoszcz

1. Data: Godzina:
(dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

.....
data, podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 4 do „Polityki bezpieczeństwa „

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa i obsługi systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Małogoszcz przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

[illegible]

[illegible]

Załącznik nr 5 do „Polityki bezpieczeństwa”.

.....
/imię i nazwisko pracownika/

.....
/adres zamieszkania/

OŚWIADCZENIE

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

- a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
- b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych
- c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

.....
(podpis pracownika)

.....
(podpis złożono w obecności)

Załącznik nr 6 do „Polityki bezpieczeństwa”

.....
/miejscowość, data/

U P O W A Ż N I E N I E N r.....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

U p o w a ż n i a m

.....
/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.....
/nazwa jednostki organizacyjnej/

Upoważnienie wydaje się na czas zatrudnienia w jednostce.

.....
Administrator Danych

Załącznik nr 7 do „Polityki bezpieczeństwa”

--	--

(nazwisko i imię) (stanowisko)

L.p	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	hasło	Uwagi
1					
2					
3					
4					

Zakres upoważnienia:

wgląd	D
wprowadzanie	W
modyfikacja	M
usuwanie	U

(Administrator Bezpieczeństwa Informacji)

.....

(imię i nazwisko)

(miejscowość, data)