ZARZĄDZENIE NR 60/2012
BURMISTRZA BIAŁEGO BORU
z dnia 24 maja 2012 r.

w sprawie ustalenia „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Białym Borze".

Na podstawie art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. nr 142, poz 1591 z późn. zm) art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3 ust.3 oraz § 4 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 z 2004r.),

zarządzam, co następuje:

§ 1. Ustala się „Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącą do przetwarzania danych osobowych w Urzędzie Miejskim w Białym Borze zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuję pracowników Urzędu Miejskiego w Białym Borze do stosowania zasad określonych w „Polityce bezpieczeństwa".

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Traci moc Zarządzenie nr 89/09 Burmistrza Białego Boru z dnia 01 września 2009 r.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Franciszek Lech Kwaśniewski

Załącznik
do zarządzenia Nr 60/2012
Burmistrza Białego Boru
z dnia 24.05.2012 r.

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

w Urzędzie Miejskim w Białym Borze

Opracowali: Bożena Pankiewicz-Ginda – Sekretarz Gminy
Grzegorz Bernat - Administrator Bezpieczeństwa Informacji

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Miejskim w Białym Borze. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Białym Borze", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18 poz. 162) oraz § 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, poz. 1024).

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 Urzędu Miejskiego w Białym Borze.

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.

4. **Administrator danych, którym jest Burmistrz, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej "Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa".**

5. "Administrator bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   3) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych

osobowych i osób przy nim zatrudnionych.

6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

ROZDZIAŁ I

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, płytach w formie niezabezpieczonej itp.

ROZDZIAŁ II

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm haseł jako narzędzie umożliwiające bezpieczne uwierzytelnienie. Administrator bezpieczeństwa informacji przydziela hasła użytkownikowi, który uzyskał dostęp do korzysta z systemu informatycznego.
2. Hasła generuje administrator systemu informatycznego. Hasło i login jest przekazywane użytkownikowi w formie ustnej (hasło należy zapamiętać). Nadane hasło zostaje zapisane w rejestrze haseł i loginów prowadzonym przez Administratora danych. Wzór rejestru stanowi **zał. Nr 6** do niniejszej Polityki Bezpieczeństwa, wzór upoważnienia do przetwarzania danych osobowych stanowi **zał. nr 7** do niniejszej Polityki Bezpieczeństwa.
3. W systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu.

4. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymuszający bezpieczne zarządzanie identyfikatorami i hasłami użytkowników. Ze względu na to:

   a) raz użyty identyfikator użytkownika nie może być nadany innym osobom,
   b) zabrania się ujawniania haseł jakimkolwiek osobom trzecim,
   c) zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim,
   d) hasła są zmieniane przez Administratora danych co najmniej raz na 6 m-cy,
   e) każdy użytkownik powinien zadbać aby na jego stanowisku komputerowym zostało ustawione przez Administratora hasło startowe (bios) i aby było ono aktywne tzn. istniała konieczność jego poprawnego wpisania w celu uruchomienia komputera,
   f) niedopuszczalnym jest samodzielna nieuprawniona próba zmiany lub zmiana przez użytkowników nie będących administratorami, danych pozwalających uzyskiwać dostęp do zasobów systemowych innym użytkownikom,
   g) po ustaniu zatrudnienia lub po odebraniu uprawnienia osobie przetwarzającej dane administratorzy powinni blokować użytkownika (identyfikator) w systemie informatycznym, aby uniemożliwić zalogowanie się do systemu.

ROZDZIAŁ III

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego pracownika po zatwierdzeniu przez administratora bezpieczeństwa informacji i jest wykonywana przez administratora systemu.
2. Wyrejestrowanie lub zmiana uprawnień użytkownika następuje na wniosek przełożonego danego pracownika przez administratora bezpieczeństwa informacji. Wyrejestrowanie może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
5. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest
   a) nieobecność w pracy trwająca dłużej niż 30 dni kalendarzowych,
   b) zawieszenie w pełnieniu obowiązków służbowych,
   c) zwolnienie z pełnienia obowiązków służbowych.
6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.
7. Pracownik opuszczający stanowisko pracy z komputerem nawet na chwilę, zobowiązany jest wylogować się z systemu informatycznego służącego do przetwarzania danych. Powinien również dodatkowo wylogować się z systemu operacyjnego.

ROZDZIAŁ IV

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, sposób, miejsce i okres przechowywania

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 systemów 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 kasie pancernej USC.
5. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny, tak by nie można było użyć ich ponownie.
6. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
7. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności. W zależności od rodzaju przechowywanych informacji określany jest wymagany czas przechowywania nośników danych osobowych, wydruków, jak również danych osobowych w systemie informatycznym.
8. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
9. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
10. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.
11. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp..
12. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

ROZDZIAŁ V

Sposób zabezpieczenia danych osobowych

1. 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.

2. 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 ppkt. 1),
   3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

3. 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.

4. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa w Urzędzie Miejskim w Białym Borze" 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.

5. Wykaz pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Urzędu Miejskiego w Białym Borze i ich zabezpieczeń zawiera załącznik **nr 1** do niniejszej Polityki Bezpieczeństwa.

6. W celu ochrony przed utratą danych w Urzędzie Miejskim w Białym Borze stosowane są następujące zabezpieczenia:
   1) zastosowanie listew przepięciowych,
   2) ochrona serwerów i komputerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
   3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach CD lub odrębnych dyskach twardych, z których w przypadku awarii odtwarzane są dane i system operacyjny. Użytkownik winien sam zadbać o archiwizację danych wytworzonych przez siebie typu (zdjęcia, pisma, pocztę wychodzącą i przychodzącą). Administrator archiwizuje dane systemów oraz innych programów zainstalowanych na serwerze do użytku ogólnego lub częściowego,
   4) w przypadku, gdy na stanowisku komputerowym nie jest zainstalowany program antywirusowy lub nie jest aktualny, nie należy wkładać ani podłączać wymiennych nośników danych (dyskietek, płyt, pendrive itp.) ani korzystać z internetu (w przypadku gdy subskrypcja na aktualizację oprogramowania antywirusowego dobiega końca, należy powiadomić Administratora,
   5) ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.

7. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu. 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,

8. 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 podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewal sprzętowy, 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. Zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.
W efekcie zapewnione jest:

- *zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,*
- *filtrowanie pakietów i blokowanie niektórych usług*
- *objęcie ochroną antywirusową wszystkich danych ściąganych z internetu na stacjach lokalnych,*
- *zapisywanie logów połączeń użytkowników z siecią Internet,*
- *zastosowanie programów anty szpiegowskich i anty wirusowych.*

9. Postanowienia końcowe.
    - do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami.
    - zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.
    - osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych
    - w pomieszczeniach w których znajdują się serwery zamontowane są czujniki dymu.
    - w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego
    - w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.
    - większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.
    - w godzinach pracy, w czasie nieobecności pracowników w biurze, pomieszczenia w których przetwarzane są dane należy zamykać na klucz, po zakończeniu pracy komputer należy wyłączyć.
    - wykaz pomieszczeń w budynku Urzędu Miejskiego w Białym Borze tworzących granice obszarów, osoby i referaty, które przetwarzają dane osobowe oraz wskazanie przetwarzanych danych osobowych z uwzględnieniem programów komputerowych stanowi **zał. nr 1** do niniejszej Polityki Bezpieczeństwa.
    - opis struktur zbiorów danych stanowi **zał. Nr 2** do niniejszej Polityki Bezpieczeństwa.
    - po godzinach pracy ostatnia osoba opuszczająca budynek Urzędu zobowiązana jest zabezpieczyć pomieszczenia i budynek w sposób uniemożliwiający wejście osób nieuprawnionych tj. zamknąć budynek na wszystkie zainstalowane zamki.

ROZDZIAŁ VI

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Prace serwisowe mogą być wykonywane wyłącznie w siedzibie Urzędu. W przypadku uszkodzenia zestawu komputerowego nośnik informacji danych na których są przechowywane dane osobowe zostaje zabezpieczony przez administratora systemu informatycznego przed dostępem osób nieuprawnionych.

2. Pracownicy winni zgłaszać wszelkie niesprawności systemu informatycznego zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych".

3. W przypadku konieczności przeprowadzenia prac serwisowych poza siedzibą urzędu dane z naprawianego urządzenia muszą zostać w sposób trwały usunięte. Od poniższego wymagania możliwe jest odstępstwo, jeżeli urządzenie, podczas przechowywania poza siedzibą przedsiębiorstwa, będzie pod stałym nadzorem osoby upoważnionej do dostępu do danych na nim przetwarzanych, wskazanej przez administratora bezpieczeństwa informacji.

4 Administrator bezpieczeństwa informacji wykonuje okresowy przegląd zbioru danych osobowych oraz usuwa dane, których przechowywanie jest dłużej nieuzasadnione.

ROZDZIAŁ VII

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 VIII

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:

- zabezpieczenia systemu informatycznego,
- technicznego stanu urządzeń,
- zawartości zbioru danych osobowych,
- ujawnienia metody pracy lub sposobu działania programu,
- jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
- innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, 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:
- 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,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,
- 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:
   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   - rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora danych,
   - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

6. 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.

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

8. 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.

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

10. 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 IX

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 szczególna uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   b) kontrola ewidencji nośników magnetycznych,
   c) kontrola właściwej częstotliwości zmiany haseł.

ROZDZIAŁ X

Szkolenia

1. Wszyscy pracownicy mający dostęp do danych osobowych zobowiązani są znać przepisy:
   - ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy;
   - o ochronie danych osobowych wynikających z ustawy o ochronie danych

osobowych,
- o odpowiedzialności karnej za naruszenie danych osobowych

na potwierdzenie tego faktu składa się oświadczenie, stanowiące **zał. Nr 4** do niniejszej Polityki Bezpieczeństwa.

2. Wszyscy pracownicy Urzędu mają obowiązek brać udział w szkoleniach,
3. 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.

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 5** 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 Miejskim w Białym Borze" wchodzi w życie z dniem jej podpisania przez Burmistrza.

BURMISTRZ

Franciszek Lech Kwaśniewski

Załącznik nr 1 do „ Polityki bezpieczeństwa"

Wykaz pomieszczeń w budynku Urzędu Miejskiego w Białym Borze tworzących granice obszarów, osoby i referaty, które przetwarzają dane osobowe oraz wskazanie przetwarzanych zbiorów danych osobowych z uwzględnieniem programów komputerowych

POKÓJ NR 2 – piwnica - „Archiwum zakładowe" (archiwalne zbiory danych osobowych)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Sadlak Bożena - Łapiczewska Grażyna

POKÓJ NR (pomieszczenie bez numeru) – parter – Serwerownia (elektroniczna baza danych osobowych Urzędu)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Bernat Grzegorz, - Sztuba Bogumiła.

POKÓJ NR 10 – parter - „USC, Ewidencja Ludności, Dowody Osobiste" (zbiór danych ewidencji ludności, dowodów osobistych, USC, skrócone kartoteki osobowe) programy: SELWIN – ewidencja ludności, USCWin2 - USC, system do dowodów osobistych SWDO, system dowód osobistych ZMOKu.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Zielke Halina, - Bernat Grzegorz, - Sztuba Bogumiła.

POKÓJ NR 11 – parter – „Oświata" (Ewidencja awansów nauczycieli mianowanych, ewidencja realizacji obowiązku nauki, ewid. Dofinansowania nauki młodocianych pracowników). Program SIO	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Kulczyńska Teresa, - Rajnert Magdalena.

POKÓJ NR 15 – parter – „Koncesje Alkoholowe, Profilaktyka i Rozwiązywanie Problemów Alkoholowych" (Rejestr osób posiadających koncesje na sprzedaż napojów alkoholowych, rejestr osób wobec których podjęto działania o przymusowe leczenie odwykowe)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Sadlak Bożena - Łapiczewska Grażyna

POKÓJ NR 17, 18, 19, 21 – biura w podwórzu – Straż Miejska (baza programu „TRAFIC", baza programu „CEPiK", baza programu „PESELnet")	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Lada Waldemar, - Pawłowska Aniela, - Dobrzańska Anna, - Radke Paweł, - Szwajczewski Artur, - Mikuszewska Magdalena, - Orzłowski Dominik, - Priadka Piotr,

	- Geda Joanna, - Kirko Arkadiusz, - Kleban Krzysztof, - Seń Bożena, - Rząsa Adela, - Paluch Anna, - Chomiszczak Marta, - Dobrzański Andrzej, - Leman Lila, - Żyła Dorota, - Śpiewak Aleksandra, - Klatt Joanna.

POKÓJ NR 23 – I piętro – Sekretariat Burmistrza – „Rejestr Skarg i Wniosków", program e-dok (Sygnity)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Marczak Małgorzata, - Marzec Stanisława

POKÓJ NR 26 – I piętro – Sekretarz – „Oświadczenia majątkowe pracowników Urzędu oraz pracowników jednostek podległych gminie"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Pankiewicz-Ginda Bożena, - Borowicz Zdzisław.

POKÓJ NR 28, 29, 32 – I piętro - OBSŁUGA Referatu Inwestycji, Planowania Przestrzennego i Zamówień Publicznych (Rejestr decyzji o warunkach zabudowy, o lokalizacji inwestycji celu publicznego, wnioskodawców dot. planów zagospodarowania przestrzennego i studium uwarunkowań, baza zamówień publicznych)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Kostiw Władysław, - Andrusieczko Jan, - Majek Anna, - Nieckarz Krystyna.

POKÓJ NR 30, 31 – I piętro - OBSŁUGA Referatu Nieruchomości i Gospodarki Komunalnej (Ewidencja właścicieli gruntów, nabywców lokali mieszkalnych i użytkowych, rozgraniczenia nieruchomości, rejestr dzierżawców i najemców), program: WINSARCZ, iMPA.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Kwolek Marczewska Aneta, - Pańczyk Danuta, - Szcześniak Krzysztof, - Sobociński Arkadiusz.

POKÓJ NR 31, 33, 34, 35, 36,37, 38, 39 – I piętro - OBSŁUGA Referatu Finansowo – Budżetowego (System Gmina2, PŁATNIK, SCHRIMPP, ewidencja zwrotu podatku akcyzowego, ewidencja tytułów wykonawczych)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Dobrzańska Anna, - Suproń Izabela, - Gałczyńska Danuta, - Kleinszmid Marta,

	- Gabrysiak Iwona, - Marzec Stanisława, - Gregorczyk Jolanta, - Wójtowicz Jolanta.

POKÓJ NR 35 – I piętro – OC, Ochrona p-poż. (Świadczenia rzeczowe i osobiste, rejestr przedpoborowych)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Gregorczyk Jolanta, - Lisiewicz Marianna.

POKÓJ NR 40 – I Pietro – Ochrona Środowiska, Rolnictwo (Rejestr wnioskodawców o wycinkę drzew i krzewów, ewidencja zezwoleń na posiadanie psów ras uznawanych za agresywne, ewidencja azbestowa, ewidencja przydomowych oczyszczalni ścieków, ewidencja koncesji na wywóz odpadów komunalnych)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Lisiewicz Marianna, - Gregorczyk Jolanta.

POKÓJ NR 46 – II piętro – Informatyczna baza danych urzędu	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Bernat Grzegorz, - Sztuba Bogumiła.

POKÓJ NR 47 – II piętro – Rada Miejska (Oświadczenia majątkowe radnych, wykaz radnych, wybory ławników)	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Sztuba Bogumiła, - Zielke Halina.

Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	
Administrator Danych	Imię i nazwisko: - Franciszek Lech Kwaśniewski
Zastępca Burmistrza	Imię i nazwisko: - Paweł Mikołajewski
Sekretarz Gminy	Imię i nazwisko: - Bożena Pankiewicz-Ginda
Administrator Bezpieczeństwa Informacji	Imię i nazwisko: - Bernat Grzegorz
Radca Prawny	Imię i nazwisko: - Sobańska Bożena
Audytor Wewnętrzny	Imię i nazwisko: - Brak

Uwaga!

1. Obsługa techniczna urzędu (sprzątaczki, pracownicy gospodarczy podpisują oświadczenie, którego wzór stanowi zał. nr 4 do „Polityki bezpieczeństwa".
2. Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia (**zał. nr 7**) nadanego przez Administratora oraz oświadczenia (**zał. nr 4**).

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

Zbiór danych USC I 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.

Zbiór danych EWIDENCJA LUDNOŚCI zawiera następujące pola:

Dane osobowe
- nazwiska i imiona
- nazwisko rodowe i z poprzedniego małżeństwa,
- imiona rodziców,
- data urodzenia,
- miejsce urodzenia,
- akta urodzenia, data i nr USC
Dane osobowe archiwalne
- nazwiska i imiona,
- nazwisko rodowe i z poprzedniego małżeństwa.
Adres zamieszkania lub pobytu stałego oraz data zameldowania
Archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania
Adres czasowy oraz czas pobytu czasowego
Archiwalne adresy czasowe oraz okresy pobytów czasowych
Dokument tożsamości
- rodzaj dokumentu,
- seria i numer dowodu,
- wystawca dokumentu,
- rysopis :wzrost, kolor oczu, znaki szczególne;
Numer ewidencyjny PESEL

USC i nr aktu urodzenia
Stan cywilny:
- imię i nazwisko współmałżonka,
- nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
- data zawarcia małżeństwa,
- USC i numer aktu małżeństwa,
- data wydania i wydający dokument tożsamości,
Stan cywilny archiwalny
- imię i nazwisko małżonka,
- nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
- data zawarcia małżeństwa,
- USC i numer aktu małżeństwa,
Data wydania i wydający dokument tożsamości
Archiwalne dokumenty tożsamości
Obowiązek wojskowy
- czy podlega obowiązkowi,
- nazwa i nr wojskowego dokumentu tożsamości,
- stopień wojskowy,
Data zgonu, USC i numer aktu zgonu
Imiona i nazwiska rodowe
Narodowość
Obywatelstwo (data zmiany , podstawa prawna)
Adnotacje o rozwodzie

Zbiór danych „Podatki" zawiera następujące pola:

Imię i nazwisko podatnika
Adres zamieszkania
Numer NIP
Numer PESEL
Numery aktów notarialnych
Numery działek

Pozostałe zbiory danych zawierają przeważnie pola:

Imię i nazwisko
Adres zamieszkania
Numer NIP
Numer PESEL
Informacje o posiadanym majątku
Numery działek
Wykształcenie

Sposób przepływu danych pomiędzy poszczególnymi systemami określają instrukcje działania poszczególnych programów.

Załącznik nr 3 do „Polityki bezpieczeństwa „

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego
w Urzędzie Miejskim w Białym Borze

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 i podpis
Administratora Bezpieczeństwa Informacji

Załącznik nr 6 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)

Załącznik nr 7 do „Polityki bezpieczeństwa"

.....
/miejscowość, data/

U P O W A Ż N I E N I E Nr.....

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 Urzędzie Miejskim w Białym Borze
/nazwa jednostki organizacyjnej/

Upoważnienie wydaje się na czas zatrudnienia w jednostce.

.....
Administrator Danych