Załącznik
do Zarządzenia Nr 116/09
Burmistrza Trzebiatowa
z dnia 31 grudnia 2009 r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Trzebiatowie

Opracowali:
Agnieszka Słodkowska – Łopyta
Bogdan Turczyn

Spis treści:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Miejskim w Trzebiatowie. 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.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Trzebiatowie, 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 art. 36 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./ oraz § 3 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:
   a/ stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   b/ 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 Trzebiatowie.
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 Trzebiatowa, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji 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:
   a/ ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   b/ 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,
   c/ niezwłocznego informowania administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   d/ 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 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

§ 4. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Miejskiego w Trzebiatowie jest Burmistrz.

§ 5. 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.

§ 6. 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.

§ 7. 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.

§ 8. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Trzebiatowie" 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.

§ 9. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania w Urzędzie Miejskim w Trzebiatowie zawierają załączniki nr 1 i 2 do niniejszego dokumentu.

§ 10. W celu ochrony przed utratą danych w Urzędzie Miejskim w Trzebiatowie stosowane są następujące zabezpieczenia:

1/ odrębne zasilanie sprzętu komputerowego,
2/ ochrona stacji roboczych i serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
3/ ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach CD oraz taśmach magnetycznych, 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/.
5/ zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:
   a/ wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenia danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa,
   b/ 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. Formularz nadania i odebrania uprawnień stanowi załącznik nr 7,
   c/ 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.

§ 11. 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 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 loga fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią.
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,

§ 12. W zakresie bezpiecznej eksploatacji sprzętu teleinformatycznego.

1/ Wszyscy pracownicy Urzędu Miejskiego w Trzebiatowie, których stanowiska wyposażone są w komputer, mogą wykorzystywać jedynie legalne oprogramowanie z licencją wykupioną przez Urząd.
2/ Za programy zainstalowane na komputerze /inne niż urzędowe/, odpowiedzialny jest użytkownik komputera.
3/ Instalacji oprogramowania na stanowiskach pracowniczych można dokonywać jedynie z nośników znajdujących się w zasobach Urzędu, zgodnie z ilością posiadanych przez Urząd licencji. Ich instalacja może być dokonywana wyłącznie przez Informatyka Urzędu Miejskiego w Trzebiatowie.
4/ Wszyscy pracownicy przyjmują do wiadomości informacje o konieczności pracy na legalnym oprogramowaniu.

5/ Korzystanie ze **służbowych** dyskietek, płyt CD/DVD, pamięci flash oraz innych nośników wymiennych, powinno być wcześniej przeskanowane programem antywirusowym.
6/ Użytkownik odpowiada za właściwe zabezpieczenie komputera w miejscu pracy poprzez – stosowanie hasła dostępu /logowanie/wylogowanie/, w przypadku wyjścia zamknięcie pomieszczenia, a w przypadku użytkowania komputera przenośnego po zakończeniu pracy dodatkowo należy go schować do zamykanej szuflady biurka lub szafy.
7/ Zabrania się:
   a/ udostępniania stanowisk roboczych oraz istniejących na nich danych /w postaci elektronicznej jak i wydruków/ osobom nieupoważnionym;
   b/ wykorzystywania sieci komputerowej i komputerów w celach innych niż służbowych;
   c/ samowolnego instalowania i używania programów komputerowych /posiadających lub nie posiadających licencji/;
   d/ trwałego lub czasowego kopiowania programów komputerowych w całości lub części jakimikolwiek środkami i w jakiejkolwiek formie;
   e/ publicznego rozpowszechniania programów komputerowych lub ich kopii,
   f/ przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko;
   g/ udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej lub Intranetu;
   h/ wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez zgody informatyka;
   i/ używania prywatnych skrzynek mailowych działających na innych serwerach niż urzędowy;
   j/ uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści;
   k/ kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody Administratora Danych Osobowych;
   l/ zabraniam wytwarzania, przetwarzania, przechowywania informacji niejawnych w jawnych komputerach;
   m/ używania własnych prywatnych dyskietek, płyt CD/DVD, pamięci flash oraz innych nośników wymiennych;
   n/ ściągania i instalowania jakichkolwiek programów z Internetu, bez wcześniejszego porozumienia z Informatykiem;
   o/ ściągania muzyki, filmów, zdjęć, programów oraz wszelkich materiałów do użytku prywatnego;
   p/ wynoszenia komputerów przenośnych zawierające dane służbowe i dane osobowe bez wcześniejszego poinformowania informatyka /Administratora Bezpieczeństwa Informacji/.
8/ Dopuszcza się możliwość użytkowania przenośnych komputerów poza miejscem pracy w celach służbowych, przy zachowaniu wyżej wymienionych punktów, ze szczególnym uwzględnieniem dbałości o odpowiednie zabezpieczenie komputera przed ulotnością zgromadzonych na nim danych, dostępem innych osób, jak i fizycznym jego zabezpieczeniu. Użytkownik ponosi odpowiedzialność za fizyczne uszkodzenie komputera, a także za jego utratę w tym utratę danych służbowych oraz informacji zawierających dane osobowe.
9/ Naruszenie wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowi poważne naruszenie zasad pracy.

§ 13. W zakresie dostępu i wyposażenia pomieszczeń serwera.
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 przebytym szkoleniu z zakresu

ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. /Dz. U. Nr 133, poz. 883 z późn. zm./,

4/ w pomieszczeniach, w których znajdują się serwery jest zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,

5/ w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,

6/ większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

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

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

§ 16. Na podstawie zgromadzonych materiałów, o których mowa w § 15, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia administratorowi danych /Burmistrzowi/.

Rozdział 4

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 17. W przypadku stwierdzenia naruszenia:

1/ zabezpieczenia systemu informatycznego,

2/ technicznego stanu urządzeń,

3/ zawartości zbioru danych osobowych,

4/ ujawnienia metody pracy lub sposobu działania programu,

5/ jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

6/ innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych /np. zalanie, pożar, itp./

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

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

§ 19. 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.

§ 20. 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 powiadamia o zaistniałym naruszeniu administratora danych,
4/ nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

§ 21. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 5, 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.

§ 22. Raport, o którym mowa w § 21, Administrator Bezpieczeństwa niezwłocznie przekazuje administratorowi danych /Burmistrzowi/, a w przypadku jego nieobecności osobie uprawnionej.

§ 23. 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.

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

§ 25. Analiza, o której mowa w § 24, 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

§ 26. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
1/ administrator danych,
2/ Administrator Bezpieczeństwa .

§ 27. W ramach kontroli należy zwracać szczególna uwagę na:
1/ okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
2/ kontrola ewidencji nośników magnetycznych,
3/ kontrola właściwej częstotliwości zmiany haseł.

Rozdział 6

SZKOLENIA

§ 28. Wszyscy pracownicy Urzędu mają obowiązek brać udział w szkoleniach.

§ 29. Szkolenie powinno dotyczyć:
1/ obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
2/ przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział 7

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

§ 30. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.

§ 31. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

§ 32. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa .

§ 33. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.

§ 34. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 8

ARCHIWIZACJA DANYCH

§ 35. Dane systemów kopiowane są w systemie tygodniowym.

§ 36. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie.

§ 37. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa.

§ 38. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w sejfie, w kasie Urzędu.

§ 39. Kopie awaryjne przechowywane są w sejfie, w kasie Urzędu.

§ 40. Płyty CD, DVD, na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny, tak by nie można było użyć ich ponownie.

§ 41. Administrator Bezpieczeństwa odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.

§ 42. Administrator Bezpieczeństwa dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności.

Rozdział 9

POSTANOWIENIA KOŃCOWE

§ 43. 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.

§ 44. 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 6 do niniejszego dokumentu.

§ 45. 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.

§ 46. 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 /Dz. U. z 2002 r. Nr 101,

poz. 926 z późn. zm./ oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 47. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych /Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm./, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych /Dz. U. Nr 100, poz. 1024/ oraz 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. 1024/.

§ 48. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Trzebiatowie" wchodzi w życie z dniem jej podpisania przez Burmistrza.

BURMISTRZ TRZEBIATOWA

Sławomir Ruszkowski