BURMISTRZ MIASTA I GMINY
w Nakle nad Notecią

Nakło nad Notecią, dnia 30.05.2005 r.

Zarządzenie Nr 55/05
z dnia 30 maja 2005 r.
Burmistrza Miasta i Gminy w Nakle nad Notecią

w sprawie wdrożenia działań techniczno - organizacyjnych na rzecz
ochrony danych osobowych przetwarzanych
w Urzędzie Miasta i Gminy w Nakle nad Notecią

Na podstawie art. 33 Ustawy o samorządzie gminnym z dnia 8 marca 1990 r. (tekst jednolity Dz.U.01.142.1591; z późn. zm.) oraz, przepisów art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. poz. 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25 poz. 219 i Nr 33, poz. 285) oraz 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.04.100.1024) zarządzam, co następuje:

§1

W celu zapewnienia należytego bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Nakle n. Notecią, wprowadza się:

1. Politykę Bezpieczeństwa Ochrony Danych Osobowych.
2. Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią.
3. Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią.

§2

Uchyla się Zarządzenia Burmistrza Gminy Nakło nad Notecią: z dnia 30 sierpnia 1999 r., nr 31/99; z dnia 8 września 1999r. nr 32/99; z dnia 29 września 1999 r. nr 38/99.

§3

Zarządzenie wchodzi w życie z dniem podpisania.

§4

Realizację postanowień zarządzenia powierzam Kierownikom/Naczelnikom wszystkich komórek organizacyjnych i pracownikom na stanowiskach samodzielnych.

BURMISTRZ
Piotr Ventala

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią

§1

Postanowienia ogólne

Niniejsza instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią. W sprawach nieokreślonych niniejszą instrukcją należy stosować postanowienia innych instrukcji obowiązujących w Urzędzie Miasta i Gminy w Nakle nad Notecią (np. Instrukcji postępowania w przypadku naruszenia ochrony danych).

§2

Przez określenia użyte w instrukcji należy rozumieć:

1. **Dane osobowe** - każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby.
2. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów komputerowych, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne.
5. **Sieć UMiG** - sieć informatyczna łącząca systemy informatyczne w budynku lub oddziałach UMiG w Nakle n/Not,
6. **Zbiór ewidencyjny** - kartoteki, skorowidze, wykazy, księgi zawierające dane osobowe.
7. **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych.
8. **Administrator Danych Osobowych (ADO)** - **Administrator Danych** – Urząd - Burmistrz Miasta i Gminy w Nakle nad Notecią.
9. **Administrator Bezpieczeństwa Informacji (ABI)** - osoba wyznaczona przez Administratora Danych Osobowych odpowiedzialna za nadzór i przestrzeganie zasad ochrony danych osobowych w systemie informatycznym oraz w zbiorach ewidencyjnych

oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

10. **Administrator Systemu Informatycznego (ASI)** - osoba upoważniona do wprowadzania zmian w systemie informatycznym, posiadająca najwyższy poziom dostępu i uprawnienia administratora zarządzającego zasobami sieci informatycznej i kontami użytkowników.
11. **Użytkownik** - osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym, która posiada ustalony indywidualny identyfikator.
12. **Hasło** - ciąg znaków, liter, cyfr lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
13. **Serwisant** - upoważniony pracownik firmy świadczącej usługi w zakresie naprawy i konserwacji sprzętu i oprogramowania.
14. **Naruszenie ochrony danych osobowych** - naruszenie zabezpieczeń systemu informatycznego lub sytuacja, gdy stan urządzeń, zawartość zbioru danych, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie tych danych.
15. **Naruszenie zabezpieczeń systemu informatycznego** - jakiekolwiek naruszenie poufności, integralności, dostępności, autentyczności, niezawodności i bezpieczeństwa systemu informatycznego, powstałe samoistnie w systemie, bądź dokonane przez osoby nieuprawnione lub uprawnione, działające w złej wierze albo omyłkowo.

§3

Procedury nadawania uprawnień użytkownikom do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym.

1. Administrator Danych zobowiązany jest do nadania uprawnień osobie do przetwarzania danych i rejestrowania tych uprawnień w związku z realizacją przydzielonych mu zadań.
2. Utworzenie konta użytkownika dającego dostęp do systemu oraz nadanie uprawnień do bazy następuje na pisemny wniosek osoby kierującej wydziałem lub osoby na samodzielnym stanowisku zgodnie z złącznikiem nr 1.
3. Administrator Systemu Informatycznego zakłada konto użytkownika w systemie o odpowiednim identyfikatorze i prawach dostępu adekwatnych do wykonywanych obowiązków służbowych oraz dostosowuje środki techniczne i informatyczne.
4. Wykreślenie użytkownika z ewidencji osób biorących udział przy przetwarzaniu danych osobowych oraz usunięcie prawa dostępu do bazy następuje na pisemny wniosek osoby kierującej działem zgodnie z załącznikiem nr 2.

5. Administrator Danych przygotowuje dokument - Wycofanie Upoważnienia do przetwarzania danych osobowych załącznik nr 6, a następnie przekazuje do realizacji Administratorowi Systemu Informatycznego
6. Wniosek o przyznanie lub cofnięcie prawa dostępu jest przechowywany przez Administratora Systemu Informatycznego. Kopia wniosku przesyłana jest do Administratora Danych.

§4

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Nazwa konta i hasło tymczasowe do systemu jest przekazywane użytkownikowi w formie ustnej przez Administratora Systemu Informatycznego. Zmiana hasła jest wymuszona przy pierwszym zalogowaniu użytkownika.
2. Użytkownik po otrzymaniu hasła jest zobowiązany do niezwłocznej jego zmiany. Każda następna zmiana hasła następuje nie rzadziej niż co 30 dni.
3. Hasło autoryzujące do Systemu Informatycznego użytkownik wpisuje osobiście. Budowa hasła jest uzależniona od poziomu bezpieczeństwa poszczególnych baz danych:
   - - poziom podstawowy - hasło powinno składać się z co najmniej 6 znaków,
   - - poziom podwyższony i wysoki - hasło powinno składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
4. Hasła dostępu użytkowników stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi. Użytkownik nie ma prawa udostępniać i ujawniać żadnego z posiadanych lub nieaktywnych haseł.
5. Hasła, w stosunku, do których zaistniało podejrzenie o ich ujawnienie podlegają bezzwłocznie zmianie.
6. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
7. W celu zabezpieczenia awaryjnego dostępu do systemu aktualne hasło Administratora Systemu jest deponowane w sejfie. Hasło powinno być dodatkowo zabezpieczone przez przypadkowym dostępem przez zastosowanie jednorazowych zabezpieczeń, np. zaklejona koperta lub oplombowane opakowanie.

§5

Procedury rozpoczęcia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Rozpoczynając pracę na komputerze użytkownik podaje wszystkie wymagane identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie innym osobom.
2. Ustawienie monitora powinno uniemożliwiać podgląd osobom nieuprawnionym.
3. W przypadku opuszczenia stanowiska pracy, użytkownik systemu obowiązany jest zablokować stację roboczą lub wylogować się z systemu.
4. Po zakończeniu pracy przy przetwarzaniu danych osobowych użytkownik powinien prawidłowo wylogować się z systemu, wyłączyć komputer i zabezpieczyć stanowisko przed dostępem osób niepowołanych.

Procedury tworzenia kopii zapasowych zbiorów danych, w których występuje baza danych osobowych

1. Kopie bezpieczeństwa tworzone są dla wszystkich baz danych w urzędzie;
2. Tworzeniu kopii bezpieczeństwa podlegają:
    a) Baza systemu ewidencji ludności i obsługi wyborców;
    b) Baza systemu podatków;
    c) Baza systemu Kadry
    d) Baza systemu Płatnik;
    e) Baza systemu USC;
    f) Katalogi z dokumentami firmowymi, tworzonymi przez pracowników.
3. Kopie wykonywane są w systemie:
    a. całościowym dziennym dla wszystkich baz danych;
    b. całościowym miesięcznym dla dokumentów firmowych, tworzonych przez pracowników;
4. Kopie w systemie dziennym (znajdujące się na serwerze) tworzone są w sposób automatyczny na wydzielonym miejscu dysku komputera podłączonego do sieci. Kopia zostaje zapisana do katalogu zawierającego w swojej nazwie datę i czas utworzenia archiwum z przeznaczeniem do nagrania na nośnik optyczny.
5. Kopie w systemie dziennym (z bazą znajdującą się na dysku lokalnym) tworzone są samodzielnie przez uprawnionych pracowników (np. po przez uruchomienie skryptu automatycznej archiwizacji). Kopia zostaje zapisana do katalogu zawierającego w swojej nazwie datę i czas utworzenia archiwum.

§6

Sposób i czas przechowywania kopii zapasowych zbiorów danych oraz likwidacji nośników informacji

1. Kopie zapasowe wykonywane na dowolnych nośnikach zewnętrznych (CD/DVD-ROM, CD/DVD-ROM-RW), przechowywane są przez Administratora Systemu Informatycznego w pomieszczeniu wyłącznie dla niego dostępnym w zamykanej szafie metalowej oraz na serwerze.
2. Kopie zapasowe bazy systemu zarządzania, katalogów z dokumentami firmowymi, tworzonymi przez pracowników, bazy poczty e-mail oraz systemów operacyjnych wraz z oprogramowaniem na stanowiskach użytkowników, przechowywane są w pojedynczej najbardziej aktualnej wersji. Dezaktualizowane wersje podlegają likwidacji.
3. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych, należy wymontować go z komputera i fizycznie zniszczyć.
4. Likwidacji uszkodzonych, zniszczonych lub zużytych nośników magnetycznych lub optycznych oraz dysków twardych dokonuje się komisyjnie.
5. Sposób postępowania z wydrukami komputerowymi zawierającymi dane przeznaczonymi dla podmiotów zewnętrznych musi być zgodny z zasadami obsługi kancelaryjnej.
6. Wydruki ze zbiorów danych tworzone i użytkowane do celów operacyjnych przez czas wykorzystywania przechowywane są w zamykanych odpowiednich szafach.
7. Likwidacja wydruków dokonuje się przy użyciu przeznaczonych do tego celu urządzeń - niszczarek lub innych urządzeń, których działanie powoduje nieodwracalne zniszczenie dokumentów uniemożliwiając odtworzenie informacji w nich zawartych.
8. W przypadku przekazywania nośników informacji podmiotom zewnętrznym lub ich przewożenia poza obszarem Urzędu Miasta i Gminy w Nakle nad Notecią należy zabezpieczyć dane przed dostępem osób nieuprawnionych stosując hasła lub kodowanie.

§7

Ochrona antywirusowa

1. Zabezpieczenie antywirusowe obejmuje:
   a) wszystkie komputery podłączone do dowolnej z sieci UMiG;
   b) komputery biorące udział w przetwarzaniu danych osobowych.
2. Oprogramowanie antywirusowe oraz baza sygnatur wirusów są systematycznie uaktualniane.
3. Każde stanowisko podłączone do sieci publicznej, które bierze udział w przetwarzaniu danych osobowych przeprowadza automatyczną aktualizację bazy wirusów raz dziennie.
4. Obowiązuje całkowity zakaz wykorzystywania własnych nośników magnetycznych lub optycznych oraz wprowadzania do komputerów oprogramowania z Intemetu.
5. Nośniki przekazywane drogą służbową należy sprawdzić za pomocą oprogramowania antywirusowego zainstalowanego na stacji roboczej lub przekazać do sprawdzenia Administratorowi Systemu Informatycznego.
6. W przypadku nieprawidłowości działania systemu z podejrzeniem o infekcję wirusami komputerowymi, użytkownicy natychmiast powiadamiają Administratora Systemu Informatycznego

§8

Konserwacja i naprawa systemu

1. Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania autoryzowanych firm zewnętrznych są wykonywane przez uprawnionych przedstawicieli tych firm (serwisantów), pod nadzorem Administratora Systemu Informatycznego bez możliwości dostępu do danych.
2. W przypadku konieczności dostępu do danych przez serwisantów, podpisują oni specjalny dokument o zachowaniu poufności (załącznik nr 8). Kopia dokumentu przesłana jest do Administratora Bezpieczeństwa Informacji (ABI).
3. Urządzenia komputerowe, dyski twarde lub inne nośniki danych przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych lub naprawia pod nadzorem Administratora Systemu Informatycznego lub osoby przez niego upoważnionej.

§9

Sposób postępowania w sytuacjach awarii systemu

Sposób postępowania w sytuacjach awaryjnych dla systemu, związanych z możliwością naruszenia ochrony zbiorów danych, regulują przepisy zawarte w dokumencie „Instrukcje postępowania w przypadku naruszenia ochrony zbiorów danych w Urzędzie Miasta i Gminy w Nakle nad Notecią".

§10

Sposób postępowania w zakresie komunikacji w sieci komputerowej

Urządzenia komputerowe (jednostki centralne, monitory, modemy) są podłączone do wydzielonej sieci elektrycznej. Żadne inne urządzenie elektryczne (czajnik, radia, wentylatory, niszczarki, kopiarki itp.) nie mogą być podłączone do tej sieci nawet, jeśli nie stanowią dużego obciążenia sieci elektrycznej.

Wszystkie zmiany dotyczące oprogramowania, użytkowników sieci oraz parametrów eksploatacyjnych (np. nazw, adresów sieciowych, oprogramowania) mogą być dokonywane wyłącznie przez Administratora Systemu Informatycznego.

Do sieci lokalnej podłączona jest sieć Intenet za pomocą wydzielonego serwera internetowego opartego na systemie operacyjnym typu Unix, dokonującego translacji adresów sieciowych (NAT) i stanowiącego dodatkowe zabezpieczenie przed dostępem z zewnątrz (firewall). Wszelkie pliki zawierające w swej treści dane osobowe przesyłane na zewnątrz sieci wewnętrznej przez łącza publiczne muszą być zaszyfrowane metodą kryptograficzną.

§11

Zasady korzystania z komputerów przenośnych

1. Komputery przenośne, używane do przetwarzania danych, powinny być zabezpieczone podczas transportu oraz zabezpieczone przed dostępem osób nieuprawnionych.
2. W szczególności należy:
    a) zabezpieczyć dostęp do komputera hasłem (gdy jest zainstalowany system Windows 95 lub 98 hasłem dostępu na poziomie BIOS),
    b) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych,

c) pliki z danymi należy zaszyfrować bądź chronić hasłem.

§12

Postanowienia końcowe

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy pracownik powinien być zaznajomiony z przepisami dotyczącymi ochrony danych osobowych oraz z niniejszą Instrukcją oraz złożyć stosowne oświadczenie dotyczące znajomości jej treści zgodnie z załącznikiem nr 7.
2. Osoba upoważniona do przetwarzania danych za naruszenie obowiązków, wynikających z niniejszej Instrukcji i przepisów o ochronie danych ponosi odpowiedzialność przewidzianą w Regulaminie Pracy oraz Kodeksie Pracy, za ciężkie naruszenie podstawowych obowiązków pracowniczych, gdy naruszenia dopuścił się pracownik.
3. Użytkownik nie przestrzegający zasad określonych w niniejszej Instrukcji ponosi odpowiedzialność karną przewidzianą w Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.), Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych - tajemnica służbowa (Dz.U. Nr 11, poz.95 z późn. zm.)

BURMISTRZ
Piotr Centala

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią

§1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią.

§2

Przez użyte w Instrukcji określenia należy rozumieć:

1. **dane osobowe** - każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby.
2. **zbiór danych osobowych** – każdy, posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3. **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
4. **zbiór ewidencyjny** - kartoteki, skorowidze, wykazy, księgi zawierające dane osobowe
5. **przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych,
6. **Administrator Danych Osobowych – Administrator Danych** - Urząd - Burmistrz Miasta i Gminy w Nakle nad Notecią,
7. **Administrator Bezpieczeństwa Informacji** - osoba wyznaczona przez Administratora Danych Osobowych odpowiedzialna za nadzór nad wdrożeniem ochrony danych osobowych w systemie informatycznym i zbiorach ewidencyjnych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
8. **Administrator Systemu Informatycznego** - osoba upoważniona do wprowadzania zmian w systemie informatycznym, posiadająca najwyższy poziom dostępu i uprawnienia administratora zarządzającego zasobami sieci informatycznej i kontami użytkowników.
9. **Osoba zatrudniona w celu przetwarzania danych osobowych** - osoba przetwarzająca dane na podstawie wydanego imiennego upoważnienia.

§3

Instrukcja określa tryb postępowania w przypadku, gdy stwierdzono naruszenie zabezpieczeń systemu informatycznego, stanu urządzeń za pomocą których przetwarzane są dane osobowej i ujawnione metody pracy, sposób działania lub jakość komunikacji w sieci telekomunikacyjnej oraz zbiorów ewidencyjnych (kartotek, skorowidzów, ksiąg, wykazów zawierających dane osobowe) mogą wskazywać na naruszenie zabezpieczeń tych danych.

§4

Każda osoba pracująca lub przebywająca na stażu itp. w Urzędzie Miasta i Gminy w Nakle nad Notecią, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym oraz zbiorach ewidencyjnych, powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub Administratora Bezpieczeństwa Informacji.

Osoba uczestnicząca przy przetwarzaniu danych osobowych, która uzyskała informacje lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym lub zbiorach ewidencyjnych, zobowiązana jest niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji, a w przypadku jego nieobecności - bezpośrednio Administratora Danych Osobowych.

§5

Administrator Bezpieczeństwa Informacji powinien w pierwszej kolejności:

1. Zapisać wszelkie informacje związane z danym zdarzeniem, a szczególnie dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu.
2. Na bieżąco wygenerować i wydrukować, (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem.

   W przypadku naruszenia dotyczącego danych osobowych przetwarzanych w zbiorach ewidencyjnych (wykonania „nieuzasadnionej" kopii, zagubienia, przekazania osobie nieuprawnionej, pozostawienia dokumentu do wglądu osób innych niż upoważnione) sporządzić notatkę zawierającą dokładny czas zdarzenia, osobę zgłaszającą wykrycie faktu oraz okoliczności powstania naruszenia ochrony danych osobowych.

3. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.

§6

Niezwłocznie należy podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, szczególnie przez:

1. Fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
2. Wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych osobowych,
3. Zmianę hasła konta administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

§7

Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego bądź zbioru ewidencyjnego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.

§8

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba powinna sprawdzić:

1. Stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
2. Zawartość zbioru danych osobowych,
3. Sposób działania programu,
4. Jakość komunikacji w sieci telekomunikacyjnej,
5. Jak również wykluczyć możliwość obecności wirusów komputerowych.

§9

Po dokonaniu powyższych czynności Administrator Bezpieczeństwa Informacji powinien przeprowadzić szczegółową analizę systemu informatycznego obejmującego identyfikacją:

- rodzaju zaistniałego zdarzenia,
- metody dostępu do danych osoby nieupoważnionej,
- skali zniszczeń.

§10

Niezwłocznie należy przywrócić normalny stan działania systemu informatycznego, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną.

§11

Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

1. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych należy przeprowadzić dodatkowe szkolenie osób biorących udział przy przetwarzaniu danych w Urzędzie Miasta i Gminy w Nakle nad Notecią.
2. Jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe.
3. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje regulowane ustawą.
4. Jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych.
5. Jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo-programowe..

§12

Administrator Bezpieczeństwa Informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz przekazuje go Administratorowi Danych Osobowych Urzędu Miasta i Gminy w Nakle nad Notecią.

BURMISTRZ
Piotr Centola

Polityka Bezpieczeństwa i Ochrony Danych Osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią

§1

Przez określenia użyte w dokumencie należy rozumieć:

Ustawa - ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, póz. 926 i z późn. zm.),

Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024)

§2

Na podstawie art. 3 ustawy oraz §4 rozporządzenia zarządza się, co następuje:

§3

Administratorem Danych Osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią w rozumieniu ustawy o ochronie danych osobowych jest Burmistrz Miasta i Gminy w Nakle nad Notecią, zwany dalej Administratorem Danych.

Administrator Danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawniona, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator Danych realizuje zadania wynikające z Rozporządzenia MSWiA z pomocą następujących pracowników:

1. Administratora Bezpieczeństwa Informacji,
2. Działu Kadr,
3. Działu Obsługi Informatycznej (Administrator Systemów Informatycznych/Informatyk),
4. Osób zajmujących kierownicze stanowiska wydziałów (Naczelnicy/Kierownicy wydziałów oraz samodzielne stanowiska)

§4

Zgodnie z wymogami art.36 ust.3 Ustawy Administrator Danych wyznacza osobę zwaną dalej "Administratorem Bezpieczeństwa Informacji", nadzorującą przestrzeganie zasad ochrony, o których mowa w ust. 1 art. 36 Ustawy.

Wyznaczenie Administratora Bezpieczeństwa Informacji ma formę pisemną zgodnie z załącznikiem nr 1, natomiast odwołanie zgodnie z załącznikiem nr 2.

§5

1. Administrator Bezpieczeństwa Informacji zobowiązany jest do:

   - prowadzenia ewidencji budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, zgodnie z załącznikiem nr 4 do niniejszego dokumentu; na podstawie ewidencji pomieszczeń oraz funkcji jakie pełnią wydzielane są odpowiednie strefy zróżnicowane pod względem zabezpieczeń dostępu do nich (załącznik nr 3),

   - prowadzenia wykazu zbiorów danych osobowych, w przypadku danych elektronicznych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zgodnie z załącznikiem nr 5 do niniejszego dokumentu,

   - utworzenia opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (załącznik nr 6),

   - utworzenia opisu sposobu przepływu danych pomiędzy poszczególnymi systemami (załącznik nr 7),

   - określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i integralności przetwarzanych danych, które opisuje dokument „Środki techniczne i organizacyjne niezbędne dla zapewnienia bezpieczeństwa przetwarzanych danych ",

   - prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów (załącznik nr 8),

   - prowadzenia wykazu dostępu do poszczególnych baz danych przez dla pracowników działów (załącznik nr 9),

   - nadzorowania przestrzegania „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią ",

2. Pracownik Działu Kadr zobowiązany jest do uzupełniania akt osobowych pracowników zatrudnionych przy przetwarzaniu danych osobowych o oświadczenia, z których wynika, że zapoznali się z przepisami obowiązującymi w tym zakresie.

BURMISTRZ
Piotr Centała

Środki techniczne i organizacyjne niezbędne dla zapewnienia bezpieczeństwa przetwarzanych danych w Urzędzie Miasta i Gminy w Nakle nad Notecią

A. Środki techniczne

1. Budynek, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest chroniony przez system alarmowy wyposażony w fotokomórki w budynku – połączony z posterunkiem Policji.
2. Urządzenia służące do przetwarzania danych osobowych znajdują się w zamkniętych pomieszczeniach.
3. Dokumenty z danymi osobowymi znajdują się w odpowiednich szafach i sejfach zamykanych na klucz.
4. W pomieszczeniach, w których znajdują się oraz są przetwarzane dane osobowe wyposażone są w urządzenia elektryczne wyposażono w urządzenia przeciwpożarowe.

B. Środki organizacyjne

1. Kierownik/Naczelnik wydziału winien przekazać Administratorowi Bezpieczeństwa Informacji wykaz osób zatrudnionych przy przetwarzaniu danych osobowych określonego zbioru.
2. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem ich do przetwarzania tych danych zostaną przeszkolone i podpisują:
   a) Prośbę o nadanie dostępu do bazy danych wraz z podaniem identyfikatora (załącznik nr 1 Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią)
   b) Upoważnienie do przetwarzania danych osobowych (załącznik nr 2 Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią)
   c) Oświadczenie o znajomości przepisów dotyczących przetwarzania danych osobowych (załącznik nr 7 Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią)
   d) Zobowiązanie do zachowania danych w tajemnicy (załącznik nr 8 Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią)
3. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzaniu danych osobowych, zgodnie z formularzem stanowiącym załącznik nr 8 Polityki Bezpieczeństwa i Ochrony Danych Osobowych

4. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych zaznajamiane z obwiązującymi przepisami o ochronie danych osobowych, procedurami przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.
6. Tymczasowe wydruki z danymi osobowymi po ustaniu ich przydatności są niszczone w niszczarkach lub w sposób uniemożliwiający odczytanie zawartych w nich danych.
7. Wyznaczono administratora bezpieczeństwa informacji Zarządzeniem Burmistrza nr 55/05 z dnia 30 maja 2005 r.
8. Ustalono dokument - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią
9. Ustalono dokument - Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Nakle nad Notecią.

C. Środki informatyczne

1. Każdy komputer wyposażono w program antywirusowy.
2. Każdy komputer posiadający dostęp do Internetu dodatkowo wyposażono w „Firewall"
3. Oprogramowanie służące do odbierania/wysyłania poczty email dodatkowo wyposażono program AntySpam (współgrający z programem Antywirusowym) w celu filtracji poczty.
4. Dostęp do zasobów Serwera w sieci lokalnej dostępny jest jedynie dla użytkowników należących do domeny po uwierzytelnieniu na Serwerze.
5. Dostęp do określonych zasobów - danych na Serwerze zależny jest od przyznanych uprawnień oraz przynależności do określonych grup użytkowników w domenie, w których to w skład wchodzą określone wydziały lub pojedyncze osoby.
6. Kopie baz danych (w tym osobowych) wykonywane są automatycznie codziennie po godzinach pracy urzędu.

BURMISTRZ
Piotr Ventala