ZARZĄDZENIE Nr K/14/2012
Burmistrza Łobżenica
z dnia 08.10.2012 r.

w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim Gminy Łobżenica ”

Na podstawie § 3 ust. 3 oraz § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004 r. Nr 100, poz. 1024),

zarządza się, co następuje:

§1. Ustala się „Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim Gminy Łobżenica” zwaną dalej „Polityką bezpieczeństwa”, która stanowi załącznik do niniejszego zarządzenia.

§2. Zobowiązuje się pracowników Urzędu Miejskiego Gminy Łobżenica do stosowania zasad określonych w „Polityce bezpieczeństwa”.

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Eugeniusz Ceriak

Załącznik do Zarządzenia Nr K/14/2012
Burmistrza Łobżenicy. z dnia 08.10.2012r.

POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM GMINY ŁOBŻENICA

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Miejskim Gminy Łobżenica. 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 systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim Gminy Łobżenica", 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 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011r. Nr 159 poz. 948) 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 Gminy Łobżenica .
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.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (jt.Dz. U. z 2001r. Nr 101, poz. 926 z późn. zm.),
2) ustawą o ochronie informacji niejawnych z dnia 1 sierpnia 2010r. (Dz. U. Nr 182, poz. 1228
1. rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159 poz. 948).

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

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 i zakłócenia ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
3. **zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenie 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.
4. **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 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) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   7) stwierdzenie próby lub modyfikacji danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   8) niedopuszczalna manipulacja danymi osobowymi w systemie,
   9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur 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) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
12) podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia oraz niedozwolone skasowanie lub skopiowanie danych osobowych,
13) rażące naruszenie dyscypliny 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.).

5. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Miejskiego Gminy Łobżenica jest Burmistrz Łobżenicy.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Do zastosowanych środków technicznych należy:
   1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   2) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   3) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.
4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   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.
5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim Gminy Łobżenica" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.
6. Wykaz pomieszczeń, w którym przetwarzane są dane osobowe oraz opis systemów informatycznych Urzędu Miejskiego Gminy Łobżenica i ich zabezpieczeń zawiera *załącznik nr 1 do niniejszego dokumentu.*
7. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu opisano w *załączniku nr 5 do niniejszego dokumentu.*
6. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania zamieszczono w *załączniku nr 4 do niniejszego dokumentu.*

Rozdział 3

METODY, ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Dla każdej osoby upoważnionej do przetwarzania danych osobowych Administrator Bezpieczeństwa Informacji ustala i przydziela odrębny identyfikator oraz hasło w celu zapewnienia bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym.
2. Hasło jest znane tylko użytkownikowi, który się nim posługuje.
3. Hasło jest zmieniane co najmniej co 30 dni, a o potrzebie zmiany hasła informuje system informatyczny.
4. Hasło jest zmieniane przez użytkownika także w przypadku podejrzenia lub stwierdzenia, że z hasłem mogły się zapoznać osoby trzecie.
5. Hasło jest utrzymywane w tajemnicy również po ustaniu jego ważności.
6. Odpowiedzialnym za przydzielanie haseł dla użytkowników, częstotliwość ich zmiany oraz rejestrację jest Administrator Bezpieczeństwa Informacji.
7. Użytkownik jest obowiązany:
    1. utrzymywać hasła dostępu, którymi się posługuje lub posługiwał w całkowitej tajemnicy;
    2. dołożyć wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem dostępu nawet po ustaniu jego ważności lub użycia hasła przez osoby trzecie.

Rozdział 4

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ORAZ KOPII ZAPASOWYCH

1. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania są przechowywane zgodnie z przepisami ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101 poz. 926 ze zm.) oraz ustawy z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym (Dz. U. z 2011r. Nr 123 poz. 698 ze zm.).
2. Dane przechowywane i gromadzone w pamięci komputera są zabezpieczone w chronionym i odpowiednio zabezpieczonym miejscu nośników informatycznych zakupionego oprogramowania operacyjnego, narzędziowego i aplikacyjnego.
3. Nośniki informacji, w tym kopie informatyczne i wydruki komputerowe przechowuje się w pomieszczeniach w metalowych szafach oraz meblach biurowych posiadających zamknięcia uniemożliwiające dostęp do nich osób nieuprawnionych.
4. W przypadku danych przechowywanych w innym pomieszczeniu niż określone w pkt. 1 dane przechowywane w pamięciach komputerów lokalnych na nośnikach informatycznych są archiwizowane w cyklu kilkudniowym.
5. Wszystkie dane przechowywane w pamięci serwerów sieciowych na odpowiednich nośnikach informatycznych są archiwizowane w cyklu tygodniowym oraz przechowywane w odpowiednio chronionym i zabezpieczonym pomieszczeniu.
6. Kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania są wykonywane codziennie na serwerze sieciowym.
7. Kopie zapasowe po ustaniu ich użyteczności są bezzwłocznie usuwane.
8. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.
9. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
10. Serwer sieciowy powinien być zabezpieczony na dwóch dyskach lustrzanych, czemu ma służyć instalacja systemu. Jego użycie zwiększa odporność na awarie, wydajność transmisji danych oraz wpływa na powiększenie przestrzeni dostępnej jako jedna całość.

Rozdział 5

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZANIA DANYCH OSOBOWYCH

11. Administrator danych (Burmistrz) 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.
12. Administrator Bezpieczeństwa sporządza półroczne plany kontroli zatwierdzone przez Burmistrza i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
13. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych (Burmistrzowi).

Rozdział 6

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. 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:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, i 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 stosowane do objawów i komunikatów towarzyszących naruszeniu,
   5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   7) udokumentować wstępnie zaistniałe naruszenie,
   8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.
4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora danych,
   4) nawiązuje bezpośredni kontakt, jeśli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 2, który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) określenie czasu i miejsca naruszenia i powiadomienia,
   3) określenie okoliczności towarzyszących i rodzaju naruszenia,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
6. Raport, o którym mowa w ust. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych (Burmistrzowi), a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez kierownictwo Urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.
9. Analiza, o której mowa w ust. 8, 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 7

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy i konserwacje sprzętu komputerowego wynikające z obciążenia sprzętu komputerowego, warunków zewnętrznych, w których eksploatowane są dane urządzenia oraz ważności sprzętu dla funkcjonowania całości systemu informatycznego są dokonywane przez Administratora Bezpieczeństwa Informacji.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych firm zewnętrznych, zostają pozbawione zapisów pod nadzorem osoby upoważnionej przez Administratora.
3. Wydruki komputerowe są bezzwłocznie usuwane po ustaniu ich użyteczności w szczególności poprzez zniszczenie ich w sposób trwały, tj. za pomocą niszczarki.
4. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie niszcząc je w sposób trwały, tj. mechaniczny.
5. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
6. Trwałego zniszczenia zbędnych nośników i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

Rozdział 8

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 3* 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 (jt. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) 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 (jt. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004 r. Nr 100, poz. 1024)
6. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim Gminy Łobżenica" w chodzi w życie z dniem jej podpisania przez Burmistrza Łobżenica .

BURMISTRZ

mgr Eugeniusz Cerlak

Załącznik nr 1
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych osobowych
w Urzędzie Miejskim Gminy Łobżenica

WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE, OPIS SYSTEMÓW INFORMATYCZNYCH W URZĘDZIE MIEJSKIM GMINY ŁOBŻENICA I ICH ZABEZPIECZEŃ

1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

NR POKOJU	OPIS SYSTEMU INFORMATYCZNEGO
KOMÓRKA ORGANIZACYJNAŁ	
STANOWISKO PRACY	
STANOWISKO PRACY	
STANOWISKO PRACY	
URZĄD STANU CYWILNEGO	

2. Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych.

NAZWA ZBIORU DANYCH	NR REJESTRU (GIODO)	PROGRAM DO PRZETWARZANIA DANYCH

3. W celu ochrony przed utratą danych w Urzędzie Miejskim Gminy Łobżenica stosowane są następujące zabezpieczenia:
   1) odrębne zasilanie sprzętu komputerowego,
   2) ochrona serwera – UPS,
   3) ochrona poszczególnych jednostek – UPS,
   4) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na taśmach magnetycznych, z których w przypadku awarii odtwarzane są dane i system operacyjny,
   5) ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.

4. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:
   1) w systemie informatycznym Urzędu zastosowano podwójną autoryzacje użytkownika,
   2) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa, który przydzieli odpowiednie uprawnienia.

5. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet:
   1) filtrowanie pakietów i blokowanie niektórych usług,
   2) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów.

6. Postanowienia końcowe:
   1) zabezpieczenie przed nieuprawnionym dostępem do danych prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
   2) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (jt Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.),
   3) w pomieszczeniu w którym znajduje się serwer zamontowano czujnik dymu oraz czujniki ruch,
   4) w pobliżu wejścia do pomieszczenia z serwerem i innymi urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.

BURMISTRZ

mgr Eugeniusz Cerlak

Załącznik nr 2
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych osobowych
w Urzędzie Miejskim Gminy Łobżenica

WZÓR

RAPORT
Z NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO W URZĘDZIE MIEJSKIM GMINY ŁOBŻENICA

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

   .....

   .....

BURMISTRZ
mgr Eugeniusz Cerlak
.....
(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 3
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych osobowych
w Urzędzie Miejskim Gminy Łobżenica

WZÓR

WYKAZ OSÓB, KTÓRE ZOSTAŁY ZAPOZNANE Z POLITYKĄ BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM GMINY ŁOBŻENICA

Przyjąłem(am) do wiadomości i stosowania zapisy „Polityki bezpieczeństwa"

Nazwisko i Imię	*Komórka organizacyjna*	*Data, podpis*

BURMISTRZ
mgr Eugeniusz Cerlak

ŁOBŻENICA, dnia .....

Procedury tworzenia kopii zapasowych danych w Urzędzie Miejskim Gminy Łobżenica

1. W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych w Urzędzie Miejskim Gminy Łobżenica, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach danych w Urzędzie Miejskim Gminy Łobżenica w oparciu o architekturę klient – serwer. Wynika stąd praktyka przetwarzania danych w bazach danych na dedykowanych dla systemu/aplikacji serwerach.

2. Jeśli stosowane dotychczas rozwiązania nie są zgodne z architekturą klient – serwer, to należy zapewnić możliwość przechowywania gromadzonych za ich pomocą danych na wyznaczonym serwerze plików.

3. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Urzędu Miejskiego Gminy Łobżenica, stanowią jedynie końcówki klienckie systemu komputerowego.

4. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach.

5. W szczególnych przypadkach, za zgodą ABI, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych.

6. Opisywana tu zasada przetwarzania danych wpływa bezpośrednio na zagadnienia związane z tworzeniem kopii bezpieczeństwa systemów.

7. Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są:
   1) w cyklu dobowym (w godzinach nocnych) za pomocą aplikacji tworzone są pełne kopie baz danych oraz aplikacji,
   2) w cyklu miesięcznym (raz w miesiącu) są wykonywane kopie na zewnętrznym dysku.

8. Zasady przechowywania kopii :
   1) Kopie zapasowe zbioru danych oraz oprogramowania i narzędzi programistycznych zastosowanych do przetwarzania danych są przechowywane w sejfie (w Urzędzie Miejskim Gminy Łobżenica).
   2) Dostęp do kopii szafy mają tylko upoważnieni pracownicy, tj. ASI oraz ABI, czas przechowywania kopii zapasowych określony został na 3 lata z kopii miesięcznych, kopie dzienne są kasowane raz w miesiącu.

Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów w Urzędzie Miejskim Gminy Łobżenica

1.Procedura rozpoczęcia pracy :

1) uruchomić komputer wchodzący w skład systemu informatycznego, podłączony fizycznie do sieci lokalnej i zalogować się podając własny identyfikator i hasło dostępu,
2) uruchomić wybrany system/aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane),
3) zalogować się do systemu/aplikacji w sposób analogiczny do przedstawionego powyżej.

2.Procedura zawieszenia pracy w systemie/aplikacji.

Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie komputera. Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem lub wylogowania się z systemu.

3.Procedura zakończenia pracy w systemie

1) zamknąć system/aplikację,
2) zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
3) wyłączyć monitor
4) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

BURMISTRZ
mgr Eugeniusz Cerlak