Zarządzenie nr 108/07
Burmistrza Czerska
z dnia 26 kwietnia 2007 r.

w sprawie wprowadzenia polityki bezpieczeństwa dla systemów teleinformatycznych używanych w Urzędzie Miejskim w Czersku

Na podstawie art. 2 ust 1 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565 z późn. zm.) oraz § 3 rozporządzenia Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212 poz. 1766)

zarządzam, co następuje:

§ 1

Wprowadza się politykę bezpieczeństwa dla systemów teleinformatycznych używanych w Urzędzie Miejskim w Czersku do realizacji zadań publicznych, określoną w załączniku do niniejszego zarządzenia.

§ 2

Wykonanie zarządzenia powierzyć Administratorowi Bezpieczeństwa Informacji w Urzędzie Miejskim w Czersku.

§ 3

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz
Marek Jankowski

RADCA PRAWNY
Grażyna Ziehlke
BU 430/84

Załącznik
do zarządzenia Burmistrza Czerska
nr 108/07 z dnia 26.04.2007 r.

POLITYKA OCHRONY DANYCH PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH URZĘDU MIEJSKIEGO W CZERSKU

§ 1

Niniejszy dokument określa:
1) sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
2) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
3) wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:
1) Urzędzie - należy przez to rozumieć Urząd Miejski w Czersku;
2) Administratorze Danych - należy przez to rozumieć Burmistrza Czerska;
3) Administratorze Bezpieczeństwa Informacji - należy przez to rozumieć Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Czersku;
4) Administratorze Systemów Informatycznych - należy przez to rozumieć Informatyka w Urzędzie Miejskim w Czersku;
5) pracowniku - należy przez to rozumieć osoby zatrudnione w Urzędzie Miejskim, a także osoby świadczące usługi na podstawie umów cywilnoprawnych;
6) danych osobowych - należy przez to rozumieć każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby;
7) przetwarzaniu danych - należy przez to rozumieć wszystkie 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) osobie trzeciej - należy przez to rozumieć każdą osobę nieupoważnioną i przez to nieuprawnioną do dostępu do danych osobowych lub zbiorów tych danych;
9) systemie informatycznym - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
10) zabezpieczeniu systemu informatycznego - należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
11) usuwaniu danych - należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
12) zbiorze danych - należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
13) sieci informatycznej (LAN) - należy przez to rozumieć lokalną sieć komputerową budynku Urzędu z końcówkami wraz ze stacjami klienckimi przyłączonymi do niej;
14) sieci telekomunikacyjnej - należy przez to rozumieć systemy transmisyjne oraz

urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju;

15) sieci publicznej - należy przez to rozumieć sieć telekomunikacyjną, nie będącą siecią wewnętrzną, służącą do świadczenia usług telekomunikacyjnych;
16) użytkowniku systemu informatycznego - należy przez to rozumieć pracownika posiadającego identyfikator i hasło do systemu informatycznego.

§ 3

1. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Miejskiego w Czersku.
2. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych powinien być zaznajomiony z przepisami o ochronie danych osobowych.

§ 4

Przetwarzanie danych może odbywać się w formie:
1) kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów;
2) systemów informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

§ 5

Informacje niejawne, które są wytwarzane, przechowywane, przetwarzane lub przesyłane przy pomocy systemów i sieci informatycznej podlegają zasadom bezpieczeństwa dostosowanym do klauzuli bezpieczeństwa. Koordynację całości spraw w tym zakresie sprawuje pełnomocnik ds. Informacji Niejawnych w Urzędzie Miejskim.

§ 6

1. Administrator Danych 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 trzecią, nieuprawnioną;
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
2. Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji nadzorującego przestrzeganie zasad ochrony danych osobowych w Urzędzie.

§ 7

Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych;
2) podejmowania stosownych działań zgodnie z niniejszym dokumentem w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia

danych znajdujących się w Urzędzie;
3) niezwłocznego informowania Administratora Danych o przypadkach narusznia przepisów ustawy o ochronie danych osobowych;
4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych;
5) przeciwdziałanie dostępowi osób trzecich do danych osobowych lub zbiorów tych danych.

§ 8

Administrator Bezpieczeństwa Informacji prowadzi ewidencję użytkowników systemu informatycznego oraz urządzeń wchodzących w jego skład.

§ 9

1. Każdy pracownik, który przetwarza dane osobowe musi mieć imienne upoważnienie nadane przez Administratora Danych do przetwarzania danych osobowych.
2. Administrator Bezpieczeństwa Informacji prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, który zawiera:
   1) imię i nazwisko osoby upoważnionej;
   2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
   3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

§ 10

1. W przypadku nieobecności Administratora Bezpieczeństwa Informacji zadania, o których mowa w § 7 realizuje Administrator Systemów Informatycznych.
2. Administrator Systemów Informatycznych składa pisemną informację z podejmowanych działań w czasie nieobecności Administratora Bezpieczeństwa Informacji.
3. W przypadku nieobecności Administratora Systemów Informatycznych jego zadania realizuje osoba upoważniona przez Administratora Danych.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

§ 11

1. Dane osobowe można przetwarzać w pomieszczeniach Urzędu do tego przystosowanych, zgodnie z niniejszym dokumentem.
2. Ze względu na szczególne nagromadzenie danych osobowych, szczególnie chronione powinny być pomieszczenia serwerowni, pomieszczenia w których przechowuje się i składuje kopie zapasowe danych osobowych, pomieszczenia archiwum zakładowego oraz pomieszczenia komórek finansowo-księgowych i kadrowo-płacowych,
3. Pomieszczenia zabezpiecza się przed dostępem osób trzecich na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
4. Przebywanie osób trzecich w obszarze, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
5. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz opis systemów informatycznych w Urzędzie zawiera załącznik nr 1 do niniejszego dokumentu.

§ 12

Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych stanowi załącznik nr 2 do niniejszego dokumentu.

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMATYCZNYCH I POWIĄZANIA MIĘDZY NIMI

§ 13

Dokładny opis techniczny zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych i powiązań między nimi znajduje się w dokumentacji oprogramowania u Administratora Systemów Informatycznych.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 14

Przepływ danych odbywa się między programami: ZUS, RADIX, USC, ARISCO, Home Banking na zasadzie wewnętrznych procedur importu i eksportu dokumentów. System Home Banking przeprowadza teletransmisje z bankiem przy pomocy łącza wdzwanialnego. Dane zaszyfrowane są za pomocą klucza wygenerowanego przez bank.

ŚRODKI TECHNICZNE I ORGANIZACYJNE SŁUŻĄCE ZAPEWNIENIU POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH

§ 15

System informatyczny, ze względu na możliwość połączenia z siecią publiczną, zapewnia środki bezpieczeństwa określone dla wysokiego poziomu bezpieczeństwa.

§ 16

1. Szczególną ochroną przed dostępem osób trzecich obejmuje się pomieszczenia, w których znajdują się serwery i węzły sieci oraz pomieszczenia, w których znajdują się zbiory danych.
2. Pomieszczenia, o których mowa w ust. 1, w czasie nieobecności pracownika powinny być stale zamknięte, a dostęp do nich powinni mieć tylko upoważnieni pracownicy.
3. Drzwi do pomieszczeń powinny być wyposażone w zamek mechaniczny.
4. Pomieszczenie serwerowni oraz miejsce przechowywania kopii danych powinny być wyposażone w odpowiedni sprzęt gaśniczy.
5. Osoby trzecie mogą przebywać w tych pomieszczeniach wyłącznie w obecności co najmniej jednego upoważnionego pracownika.
6. W trakcie prac technicznych wykonywanych przez osoby trzecie, przetwarzanie danych osobowych na wydzielonych stanowiskach jest zabronione, a sprzęt komputerowy musi być wyłączony.

§ 17

1. Urząd Miejski w Czersku wyposażony jest w elektroniczny system antywłamaniowy z całodobowym monitoringiem sygnału alarmu.
2. System alarmowy musi być objęty stałym nadzorem specjalistycznym.

§ 18

Ekrany monitorów ustawione są do wewnątrz pomieszczeń wydzielonych do przetwarzania danych osobowych, w taki sposób, by uniemożliwić wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.

§ 19

1. Obowiązkiem pracowników użytkujących komputery, w tym komputery przenośne, zawierające dane osobowe jest zachowanie szczególnej ostrożności podczas ich użytkowania, transportu lub przechowywania poza pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe, a w szczególności stosowanie ochrony kryptograficznej wobec przetwarzanych danych osobowych.
2. Używanie przez pracownika komputera przenośnego zawierającego dane osobowe poza budynkiem Urzędu Miejskiego wymaga odnotowania w ewidencji prowadzonej przez Administratora Bezpieczeństwa Informacji.

§ 20

W przypadku zdarzeń losowych (np. awaria serwera, zalanie pomieszczenia) należy zapewnić uruchomienie systemu w minimalnej konfiguracji udostępniającej zasoby systemu.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

§ 21

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie pracownik zarejestrowany w tym systemie przez Administratora Systemów Informatycznych na wniosek Administratora Bezpieczeństwa Informacji.
2. Referat Kadr i Spraw Obywatelskich Urzędu Miejskiego informuje Administratora Bezpieczeństwa Informacji o każdym nowym pracowniku, a także o ustaniu zatrudnienia lub zaprzestaniu świadczenia usług na podstawie umów cywilnoprawnych.
3. Rejestracja, o której mowa w ust. l, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu informatycznego.

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

§ 22

1. Identyfikator użytkownika systemu informatycznego:
   1) jest przydzielany przez Administratora Systemów Informatycznych na wniosek Administratora Bezpieczeństwa Informacji;

2) jest niepowtarzalny;
3) po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielany innej osobie;
4) nie podlega zmianie;
5) jest wpisywany do prowadzonej przez Administratora Bezpieczeństwa Informacji ewidencji użytkowników systemu informatycznego wraz z imieniem i nazwiskiem użytkownika systemu informatycznego;

2. Użytkownicy systemu informatycznego zobowiązani są do zachowania w tajemnicy przed osobami trzecimi ustalonych dla nich identyfikatorów.

§ 23

Hasło użytkownika systemu informatycznego:
1) jest przydzielane przez Administratora Systemów Informatycznych na wniosek Administratora Bezpieczeństwa Informacji, indywidualnie dla każdego z użytkowników systemu informatycznego, a następnie zmienione przy pierwszym zastosowaniu (zalogowaniu użytkownika systemu informatycznego) i znane tylko temu użytkownikowi systemu informatycznego;
2) nie jest zapisywane w systemie w postaci jawnej;
3) jest zmieniane nie rzadziej niż co 45 dni;
4) składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
5) jest utrzymywane w tajemnicy, również po upływie jego ważności

§ 24

1. Wyrejestrowania użytkownika systemu informatycznego z systemu informatycznego dokonuje Administrator Systemów Informatycznych na wniosek Administratora Bezpieczeństwa Informacji.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
   1) zablokowanie konta użytkownika systemu informatycznego do czasu ustalenia przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);
   2) usunięcie danych użytkownika systemu informatycznego z bazy użytkowników systemu informatycznego (wyrejestrowanie trwałe).
4. Przyczyną czasowego wyrejestrowania użytkownika systemu informatycznego z systemu informatycznego jest:
   1) nieobecność w pracy trwająca dłużej niż 21 dni kalendarzowych;
   2) zawieszenie w pełnieniu obowiązków służbowych;
   3) zwolnienie z pełnienia obowiązków służbowych.
5. Przyczyną trwałego wyrejestrowania użytkownika systemu informatycznego z systemu informatycznego jest ustanie zatrudnienia lub zaprzestanie świadczenia usług na podstawie umów cywilnoprawnych.

§ 25

1. Użytkownik systemu informatycznego odpowiedzialny jest za wszystkie czynności wykonywane przy użyciu identyfikatora i hasła użytkownika systemu informatycznego, którymi się posługuje lub posługiwał.
2. W przypadku powzięcia przez użytkownika systemu informatycznego podejrzenia lub

stwierdzenia, że z identyfikatorem lub hasłem użytkownika systemu informatycznego mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o tym Administratora Bezpieczeństwa Informacji, który zwróci się z wnioskiem do Administratora Systemów Informatycznych o nadanie nowego identyfikatora użytkownika systemu informatycznego.

§ 26

Naruszenie przez użytkownika systemu informatycznego postanowień § 25 może stanowić podstawę jego odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

§ 27

1. Rozpoczęcie pracy w systemie informatycznym odbywa się poprzez:
   1) przygotowanie stanowiska pracy;
   2) włączenie stacji roboczej;
   3) wprowadzenie swojego identyfikatora i hasła użytkownika systemu informatycznego.
2. Zakończenie pracy w systemie informatycznym odbywa się poprzez:
   1) zamknięcie aplikacji;
   2) odłączenie się od zasobów systemowych;
   3) zamknięcie systemu operacyjnego;
   4) wyłączenie stacji roboczej.
3. Zawieszenie pracy w systemie informatycznym odbywa się poprzez aktywację wygaszacza ekranu z hasłem po 15 minutach od momentu bezczynności stacji roboczej, zabezpieczenie stacji roboczej po odejściu od stanowiska lub wylogowanie z systemu informatycznego przez użytkownika systemu informatycznego.

§ 28

1. Zabrania się użytkownikom systemu informatycznego pracującym w systemie:
   1) udostępniania stacji roboczej osobom nie zarejestrowanym w systemie zgodnie z § 21;
   2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Bezpieczeństwa Informacji;
   3) używania nielicencjonowanego oprogramowania;
   4) tworzenia kopii danych na nośnikach (CD, DVD, FDD, PEN DRIVE, HDD przenośne i inne) bez zezwolenia Administratora Bezpieczeństwa Informacji;
   5) używania nośników wymienionych w pkt. 4 do wymiany informacji bez uprzedniego sprawdzenia programem antywirusowym.
2. Wykaz oprogramowania stosowanego na poszczególnych stanowiskach pracy określa porozumienie zawarte między Administratorem Danych a pracownikiem według wzoru stanowiącego załącznik nr 5.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

§ 29

1. Kopie awaryjne tworzy się z następującą częstotliwością:
   1) kopie systemu Aplikacji dla Administracji Samorządowej - codziennie, oraz dodatkowo jedna kopia z całego tygodnia;
   2) kopie pozostałych systemów informatycznych - nie rzadziej niż raz w tygodniu.
2. Kopie tworzone są automatycznie w czasie nie korzystania z danych na serwerze.
3. Kopie te wykonuje się na nośniku magnetycznym lub optycznym, które to nośniki przechowuje się w sejfie umieszczonym w pomieszczeniu innym, niż dane osobowe przetwarzane na bieżąco.
4. Kopie awaryjne podlegają takiej samej ochronie jak serwery zawierające dane osobowe.

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓWINFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ CZĘSTOTLIWOŚĆ TWORZENIA KOPIIZAPASOWYCH

§ 30

1. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
2. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
3. Administrator Systemów Informatycznych dokonuje okresowych przeglądów kopii awaryjnych i ocenia ich przydatność do odtworzenia zasobów systemu informatycznego w przypadku jego awarii.
4. Stwierdzenie utraty przez kopię awaryjną waloru przydatności do celu, o którym mowa w ust. 3, upoważnia Administratora Systemów Informatycznych do ich zniszczenia i odnotowania tego faktu.

§ 31

1. Kopie dzienne kasowane są po tygodniu.
2. Kopie tygodniowe kasowane są po miesiącu.
3. Kopie miesięczne nie są niszczone.
4. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.
5. Niszczenia kopii zapasowych na nośnikach magnetycznych dokonuje Administrator Systemów Informatycznych.

§ 32

1. Z nośników magnetycznych dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.
2. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
3. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych osobowych należy wymontować go z komputera i fizycznie zniszczyć.
4. Likwidacji wydruków dokonuje się przy użyciu przeznaczonych do tego celu urządzeń

(np. niszczarek).
5. 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, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały.
6. Trwałego zniszczenia zbędnych nośników informacji i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

SPOSOBY ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OBCEGO OPROGRAMOWANIA

§ 33

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemów Informatycznych, nie rzadziej niż raz na miesiąc, przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
4. Do obowiązków Administratora Systemów Informatycznych należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.
5. Zabrania się pracownikom blokowania pracy oprogramowania, o którym mowa w ust. 1.
6. W razie niemożności usunięcia wirusa Administrator Systemów Informatycznych ma obowiązek niezwłocznego przedstawienia Administratorowi Danych i Administratora Bezpieczeństwa Informacji lub wyznaczonej przez niego osobie, propozycji działań zaradczych. Po usunięciu wirusa Administrator Systemów Informatycznych sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności.
7. Administrator Bezpieczeństwa Informacji prowadzi rejestr przypadków obecności wirusów komputerowych w systemie i na nośnikach wykorzystywanych do przetwarzania danych osobowych w systemie.
8. Procedura, o której mowa w powyższym paragrafie, ma odpowiednie zastosowanie także do przypadków awarii systemu spowodowanych błędem programu lub użytkowników systemu informatycznego.

REJESTRACJA INFORMACJI O OSOBACH TRZECICH, KTÓRYM ZOSTAŁY UDOSTĘPNIONE DANE OSOBOWE

§ 34

Użytkownik systemu informatycznego jest obowiązany odnotować informację o udostępnieniu danych osobowych osobom trzecim, zawierającą w szczególności:
1) imię i nazwisko
2) adres zamieszkania
3) datę udostępnienia
4) zakres, w jakim udostępniono dane osobowe.

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

§ 35

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać podmiotowi nieuprawnionemu do otrzymania tych danych:
   1) do naprawy
   2) do likwidacji

   po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.
2. Urządzenia, o których mowa w ust. 1 przed ich przekazaniem pozbawia się zapisu danych osobowych.
3. Jeżeli nie jest możliwe pozbawienie urządzenia zapisu danych osobowych, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemów Informatycznych.
4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie przed przekazaniem uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 36

1. Przeglądu i konserwacji systemu Administrator Systemów Informatycznych dokonuje doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemów Informatycznych dokonuje nie rzadziej niż raz na tydzień.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe użytkownik systemu informatycznego przy współudziale Administratora Systemów Informatycznych dokonuje nie rzadziej niż raz na miesiąc.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

§ 37

Każdy pracownik Urzędu Miejskiego, który stwierdził:
1) naruszenie bezpieczeństwa systemu informatycznego,
2) naruszenie technicznego stanu urządzeń służących do przetwarzania danych osobowych,
3) naruszenie zawartości zbioru danych osobowych,
4) ujawnienie metod pracy lub sposobów działania programu osobom trzecim,
5) zmianę jakości transmisji danych w sieci telekomunikacyjnej mogącą wskazywać na naruszenie zabezpieczenia tych danych,
6) zaistnienie innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.);

obowiązany jest niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

§ 38

Do czasu przybycia Administratora Bezpieczeństwa Informacji na miejsce naruszenia ochrony danych osobowych, należy:
1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie w miarę możliwości ustalić przyczyny 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 stosownie do objawów i komunikatów towarzyszących naruszeniu w szczególności określone w instrukcjach technicznych;
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.

§ 39

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator Bezpieczeństwa Informacji w szczególności:
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 i Administratora Systemów Informatycznych.

§ 40

Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia sporządzając 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.

§ 41

1. W przypadkach naruszenia danych osobowych, o których mowa § 37, Administrator Bezpieczeństwa Informacji zobowiązuje Administratora Systemów Informatycznych do

sporządzenia raportu, którego treść stanowi załącznik nr 3 do niniejszego dokumentu.
2. Raport, o którym mowa w ust. 1, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych.
3. Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych propozycję postępowania naprawczego oraz termin wznowienia przetwarzania danych osobowych.

POSTANOWIENIA KOŃCOWE

§ 43

Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencje osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 4 do niniejszego dokumentu.

§ 44

W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy:
1) ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926);
2) 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);
3) rozporządzenia 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).

Załącznik nr 1
do polityki ochrony danych
przetwarzanych w systemach
informatycznych Urzędu Miejskiego w
Czersku

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Nr pokoju	Komórka organizacyjna	System/ program

Załącznik nr 2
do polityki ochrony danych
przetwarzanych w systemach
informatycznych Urzędu Miejskiego w
Czersku

WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMY ZATOSOWANE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nazwa zbioru (opis)	Program do przetwarzania	Obszar przetwarzania/pomieszczenie

Załącznik nr 3
do polityki ochrony danych
przetwarzanych w systemach
informatycznych Urzędu Miejskiego w
Czersku

Wzór

Raport z naruszenia bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Czersku

1. Data…….. godzina……

2. Osoba powiadamiająca o zaistniałym zdarzeniu
……
Imię, nazwisko, stanowisko służbowe

3. Lokalizacja zdarzenia……..
Nr i nazwa pomieszczenia

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące
……
……
……

5. Podjęte działania
……
……
……...

6. Przyczyny wystąpienia zdarzenia
……
……
……...

7. Postępowanie wyjaśniające
……
……
……...

……..
Data, podpis zgłaszającego

Załącznik nr 4
do polityki ochrony danych
przetwarzanych w systemach
informatycznych Urzędu Miejskiego w
Czersku

Wzór

Wykaz pracowników zatrudnionych przy przetwarzaniu danych osobowych, którzy zostali zapoznani z Polityką Bezpieczeństwa w Urzędzie Miejskim w Czersku

Przyjąłem/am do wiadomości i stosowania zapisu Polityki Bezpieczeństwa

Nazwisko i imię	Komórka organizacyjna	Data, podpis

Załącznik nr 5
do polityki ochrony danych
przetwarzanych w systemach
informatycznych Urzędu Miejskiego w
Czersku

WZÓR

Porozumienie z pracownikiem

Niniejsze porozumienie (zwane dalej „Porozumieniem") zostało zawarte w dniu _____ 200_ r. w _____ pomiędzy:
Urzędem Miejskim w Czersku, reprezentowanym przez
_____, zwanym dalej „Pracodawcą"
oraz
Panią/Panem _____, zamieszkałą/ym w _____ przy ul. _____ , zwaną/ym dalej „Pracownikiem".
Wstęp:
(A) Pracownik zatrudniony jest przez Pracodawcę na podstawie umowy o pracę zawartej w dniu _____ r.
(B) Pracodawca wyposażył stanowisko pracy Pracownika w oprogramowanie komputerowe _____, na używanie którego licencję nabył od _____ („Oprogramowanie").
Odpowiednie przepisy regulują w sposób szczegółowy zasady korzystania z Oprogramowania.
(C) Pracownik korzysta z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych.

1. Pracodawca i Pracownik uzgadniają, że do podstawowych obowiązków Pracownika należy korzystanie z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych, jak również nie korzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
2. Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny, (tekst jednolity – Dz. U. z 1997, Nr 88, poz. 553, ze zmianami) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity – Dz. U. z 2000, Nr 80, poz. 904, ze zmianami) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.
3. Pracodawca i Pracownik uzgadniają, że naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę, łączącej Pracodawcę z Pracownikiem, lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn.: Dz. U. z 1998 r., Nr 21, poz. 94, ze zm.).

Niniejsze Porozumienie zostało sporządzone w dwóch egzemplarzach, po jednym dla każdej ze stron. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.

Podpis pracownika

Podpis osoby upoważnionej do reprezentowania Pracodawcy