Urząd Miejski
ul.Kościuszki 27
89-650 Czersk

BR.0050.169.2013

Zarządzenie nr 604/13
Burmistrza Czerska
z dnia 11 grudnia 2013 r.

w sprawie wprowadzenia polityki bezpieczeństwa informacji Urzędu Miejskiego Czersk

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 ze 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.

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

§ 2.

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

§ 3.

Traci moc 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.

§ 4.

Zarządzenie wchodzi w życie z dniem podjęcia, z mocą obowiązującą od 1 stycznia 2014 r.

Burmistrz Czerska

Marek Jankowski

RADCA PRAWNY
Grażyna [illegible]
Bd 430/84

Załącznik
do Zarządzenia nr 604/13
Burmistrza Czerska
z dnia 11 grudnia 2013 r.

Polityka Bezpieczeństwa Informacji

UM CZERSK

Grudzień 2013

I. POJĘCIA PODSTAWOWE

a) **Urząd** - Urząd Miejski w Czersku;

b) **Administrator Danych** - Burmistrza Czerska;

c) **Administrator Bezpieczeństwa Informacji/ABI** - Administrator Bezpieczeństwa Informacji w Urzędzie Miasta w Czersku;

d) **Administrator Systemów Informatycznych** - Informatyk w Urzędzie Miasta w Czersku;

e) **PBI** – Polityka Bezpieczeństwa Informacji;

f) **Pracownik** - osoba zatrudniona w Urzędzie Miasta w Czersku, a także osoby świadczące usługi na podstawie umów cywilnoprawnych;

g) **Dane osobowe** - każda informacja dotycząca osoby fizycznej, pozwalającą na określenie tożsamości tej osoby;

h) **Przetwarzanie danych** - 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;

i) **Osoby trzecie** - każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych;

j) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

k) **Zabezpieczenie systemu informatycznego** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

l) **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

m) **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

n) **Sieci informatyczne (LAN)** - lokalna sieć komputerowa budynku Urzędu wraz ze stacjami klienckimi przyłączonymi do niej;

o) **Sieci telekomunikacyjne** - 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;

p) **Sieć publiczna** - sieć telekomunikacyjną, niebędącą siecią wewnętrzną, służącą do świadczenia usług telekomunikacyjnych;

q) **Użytkownik systemu informatycznego** - pracownik posiadającego identyfikator i hasło do systemu informatycznego.

r) **System tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;

s) **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą

t) **Aktywa** – Aktywa Informacyjne, mające wartość dla organizacji i podlegające ochronie;

u) **Kierownictwo Urzędu** - zgodnie z Regulaminem Organizacyjnym Urzędu, stanowią: Burmistrz, Z-ca Burmistrza, Skarbnik, Sekretarz;

v) **Poufność** - zapewnienie dostępu do informacji tylko osobom do tego upoważnionym.

w) **Integralność** - zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.

x) **Dostępność** - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.

II. DEKLARACJA KIEROWNICTWA

1. Bezpieczeństwo to stan, w którym istnieje ogół warunków organizacyjnych, prawnych i technicznych chroniących zasoby przed zagrożeniami oraz spełnienie tych warunków dla zapewnienia bezpieczeństwa Urzędu, jej pracowników i Klientów. Bezpieczeństwo to również miara zaufania, pewności do osób, podmiotów, procesów i systemów. Bezpieczeństwo to ważny instrument służący wykonywaniu przez Urząd jego zadań, które mogą okazać się zagrożone przez: działania przestępcze (włamania, napady, kradzieże, blokady dostępu do zasobów lub ich zniszczenie), awarie i błędy technologiczne, niedbalstwo i pomyłki ludzi oraz inne niewymienione formy zagrożenia.
2. Kierownictwo Urzędu jest świadome istniejących zagrożeń i ryzyka związanego z tworzeniem, przechowywaniem, przetwarzaniem i przesyłaniem informacji w tym danych osobowych. W celu ochrony informacji, minimalizacji ryzyka i przeciwdziałaniu zagrożeniom Burmistrz Miasta Czersk ustanawia niniejszą Politykę Bezpieczeństwa Informacji. Definiuje ona organizację bezpieczeństwa informacji, stosowane zabezpieczenia, zarządzanie systemami i siecią teleinformatyczną, zarządzanie ciągłością działania.
3. W związku ze znaczną wartością informacji dla Urzędu, podlega ona ochronie rozumianej, jako zapewnienie bezpieczeństwa informacji. O bezpieczeństwo informacji chronionej Urząd dba niezależnie od jej formy (elektroniczna, papierowa, słowna).
4. Kierownictwo Urzędu przez Bezpieczeństwo Informacji rozumie stosowanie, odpowiednich do zagrożeń oraz potrzeb, środków ochrony pozwalających na utrzymanie poufności, integralności i dostępności informacji przechowywanej i przetwarzanej w Urzędzie.
5. Decyzja o przyjęciu do stosowania Polityki Bezpieczeństwa Informacji ma na celu podniesienie bezpieczeństwa informacji poprzez stosowanie oraz zapewnienie odpowiednich standardów bezpieczeństwa.
6. Niniejsza Polityka Bezpieczeństwa Informacji jest adresowana do wszystkich pracowników Urzędu.
7. Kierownictwo Urzędu zapewnia środki niezbędne do skutecznej realizacji Polityki Bezpieczeństwa Informacji.

III. CEL DOKUMENTU

Polityka bezpieczeństwa informacji jest sformalizowanym i udokumentowanym zbiorem reguł oraz zasad określających zasady przetwarzania danych, a także warunki związane z zabezpieczeniem tych danych. Polityka jest podstawowym dokumentem związanym z ich ochroną.

Niniejszy dokument określa:

1) sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, 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,
3) wymagania w zakresie odnotowywania udostępniania danych i bezpieczeństwa ich przetwarzania.

Zasady Polityki Bezpieczeństwa w żadnym stopniu nie pozostają w sprzeczności z powszechnie obowiązującym prawem.

IV. ZAKRES SYSTEMU BEZPIECZEŃSTWEM INFORMACJI

1. System Bezpieczeństwa Informacji obejmuje swoim zakresem Urząd Miasta Czersk.
2. System Bezpieczeństwa Informacji obejmuje systemy informatyczne i infrastrukturę teleinformatyczną Urzędu, przetwarzanie dokumentów papierowych, archiwizację informacji na dowolnych nośnikach.
3. Niniejszy dokument nie dotyczy innych jednostek podległych Urzędowi Miasta.
4. Do przestrzegania zapisów Polityki zobowiązani są wszyscy pracownicy Urzędu.
5. W celu zapewnienia jak najwyższego poziomu bezpieczeństwa informacji, będącej w posiadaniu lub przetwarzaniu przez Urząd, do zasad wynikających z Polityki Bezpieczeństwa Informacji powinni również stosować się wszyscy dostawcy, audytorzy i konsultanci, którzy mają dostęp do informacji, dokumentów papierowych oraz zasobów i systemów informatycznych.

V. POUFNOŚĆ

Struktura informacji w Urzędzie Miasta opiera się na założeniu istnienia trzech poziomów postrzegania informacji:

Informacja jawna - informacja uznawane za powszechnie dostępne.

Informacje wewnętrzna – informacja, której przetwarzanie i udostępnianie podlega ograniczeniom z uwagi na szczególne znaczenie dla Urzędu (właściciela informacji). Informacja nie jest udostępniana publicznie za wyjątkiem sytuacji określonych prawem. Może być przekazywana na zewnątrz zgodnie z obowiązującymi przepisami prawa, ale nie jest uznawana za dostępną powszechnie. Wewnątrz Urzędu jest dystrybuowana tylko do określonych osób;

a) informacje wewnętrzne dostępne – informacje dostępne dla wszystkich pracowników Urzędu,
b) informacje wewnętrzne wrażliwe - informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
c) informacje stanowiące tajemnicę pracodawcy - informacje, których przetwarzanie i udostępnianie może narazić pracodawcę na szkodę.

Informacja niejawna - informacje, do których stosuje się przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych lub innych tajemnic prawnie chronionych.

VI. ODPOWIEDZIALNOŚĆ

1. Za ustanowienie wdrożenie i utrzymanie Polityki Bezpieczeństwa Informacji odpowiedzialny jest Burmistrz. W celu bezpośredniego nadzoru nad systemem Bezpieczeństwa Informacji powołuje on Administratora Bezpieczeństwa Informacji, na którym spoczywa odpowiedzialność za realizację Polityki.
2. Zgodnie z postanowieniami niniejszej Polityki, właściwi pracownicy Urzędu ponoszą odpowiedzialność za bezpieczeństwo informacji oraz aktywów będących w ich gestii.

BURMISTRZ / ADMINISTRATOR DANYCH

3. Administrator Danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:
   a. zabezpieczających dane przed ich udostępnieniem osobom nieupoważnionym,
   b. zapobiegających przed przekazaniem danych osobie trzeciej, nieuprawnionej,
   c. zapobiegających przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
4. Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji nadzorującego przestrzeganie zasad ochrony danych osobowych w Urzędzie.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

5. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   a. ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych,
   b. podejmowania stosownych działań w przypadku naruszeń ochrony danych osobowych, w tym przywrócenie stanu prawidłowego, zidentyfikowanie przyczyn naruszenia i osób odpowiedzialnych,
   c. niezwłocznego informowania Administratora Danych o przypadkach naruszania przepisów ustawy o ochronie danych osobowych,
   d. nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
   e. kontroli pracowników i innych osób upoważnionych pod względem wykonywania przez nich obowiązków związanych z ochroną przetwarzanych danych osobowych,
   f. przeciwdziałania dostępowi osób trzecich do danych osobowych lub zbiorów tych danych,
   g. kontroli przechowywania i archiwizacji dokumentów papierowych zawierających dane osobowe, pod względem prawidłowego zabezpieczenia tych dokumentów, ewidencji osób upoważnionych do przetwarzania danych osobowych,
   h. wykonywania audytów i monitorowania skuteczność istniejących zabezpieczeń,
   i. inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia bezpieczeństwa ochrony danych osobowych.
6. Administrator Bezpieczeństwa Informacji prowadzi ewidencję użytkowników systemu informatycznego oraz urządzeń wchodzących w jego skład.
   a. każdy pracownik, który przetwarza dane osobowe musi mieć imienne upoważnienie nadane przez Administratora Danych do przetwarzania danych osobowych. Administrator Bezpieczeństwa Informacji prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, który zawiera:

- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- login, jeżeli dane są przetwarzane w systemie informatycznym.

b. W przypadku nieobecności Administratora Bezpieczeństwa Informacji zadania, o których mowa w pkt.6, realizuje Administrator Systemów Informatycznych.

c. Administrator Systemów Informatycznych składa pisemną informację z podejmowanych działań w czasie nieobecności Administratora Bezpieczeństwa Informacji.

d. W przypadku nieobecności Administratora Systemów Informatycznych jego zadania realizuje osoba upoważniona przez Administratora Danych.

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

7. Administrator Systemów Informatycznych jest odpowiedzialny za zapewnienie bezpieczeństwa w powierzonych obszarach. W związku, z czym jest odpowiedzialny w szczególności za:
   a. ustanawianie i zapewnienie aktualności planów ciągłości działania w zakresie systemów informatycznych,
   b. okresowe testowanie aktualności i adekwatności planów ciągłości działania - monitorowanie bezpieczeństwa i wydajności środowiska IT,
   c. ustalanie i przestrzeganie zasad zapewnienia legalności wykorzystywanego oprogramowania;
   d. kontrolę legalności wykorzystywanego oprogramowania,
   e. okresowe przeglądy i konserwacje systemów i urządzeń - utrzymanie w sprawności powierzonego obszaru,
   f. zarządzanie siecią zgodnie z wymaganiami - administrację środowiskiem informatycznym w sposób zapewniający bezpieczeństwo informacji,
   g. zarządzanie uprawnieniami użytkowników w systemach,
   h. tworzenie kopii bezpieczeństwa systemów i danych zgodnie z przyjętym harmonogramem,
   i. konfigurację uprawnień użytkowników w systemach informatycznych,
   j. prowadzenie i bieżące aktualizowanie pliku „Dokumentacja IT UM Czersk".

PEŁNOMOCNIK DS. INFORMACJI NIEJAWNYCH W URZĘDZIE MIEJSKIM

8. 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.

PRACOWNICY / UŻYTKOWNICY SYSTEMU

9. Każdy pracownik Urzędu, stażysta, praktykant/użytkownik systemu, jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi zasadami ochrony informacji w swojej komórce organizacyjnej oraz w Urzędzie Miasta. Dlatego jest odpowiedzialny za znajomość i przestrzeganie zasad bezpieczeństwa informacji zawartych w PBI;

VII. INFRASTRUKTURA

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

1. System bezpieczeństwa informacji obejmuje siedzibę Urzędu Miejskiego w Czersku, przy ul. Kościuszki 27.
2. Dane osobowe można przetwarzać w pomieszczeniach Urzędu do tego przystosowanych, zgodnie z niniejszym dokumentem.
3. Ze względu na nagromadzenie danych osobowych, szczególnie chronione są pomieszczenia serwerowni, pomieszczenia, w których przechowuje się kopie zapasowe danych osobowych, pomieszczenia archiwum zakładowego oraz pomieszczenia komórek finansowo-księgowych i kadrowo-płacowych.
4. Pomieszczenia zabezpiecza się przed dostępem osób trzecich na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
5. Przebywanie osób trzecich w obszarze, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
6. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz opis systemów informatycznych w Urzędzie zawiera **Załącznik nr 1** do niniejszego dokumentu i stanowi integralną część Polityki.
7. Wykaz urządzeń i plan sieci znajdują się w pliku „Dokumentacja IT UM Czersk", stanowiącego integralna część Polityki.

INFRASTRUKTURA SPRZĘTOWA

1. Urząd prowadzi Rejestr Aktywów Systemu Bezpieczeństwa Informacji, który obejmuje następujące elementy:
   b. Komputery przenośne,
   c. Komputery stacjonarne,
   d. Serwery,
   e. Aplikacje,
   f. Dane:
      - Pliki, bazy danych i zawarte w nich informacje oraz dane umieszczone w kopiach bezpieczeństwa i archiwach umieszczanych na dowolnych nośnikach włączając w to dyski, płyty CD, DVD, pamięci USB, itp.,
   g. Infrastruktura sieciowa:
      - Okablowanie,
      - Routery z Firewall,
   h. Infrastruktura techniczna:
      - UPS,
   i. Zabezpieczenia fizyczne.

   Rejestr prowadzony jest w pliku „Dokumentacja IT UM Czersk".
2. Przegląd i aktualizacja Rejestru odbywa się nie rzadziej, niż co dwanaście miesięcy.
3. Wszystkie aplikacje, bazy danych, zasoby sieciowe, serwery plików stosowane w Urzędzie umieszczane są na serwerach dopuszczonych przez Administratora Bezpieczeństwa Informacji.
4. Zmiany dokonywane w systemie operacyjnym i/lub środowisku istotnym dla działania aplikacji mogą być wykonywane jedynie przez Administratora Systemów Informatycznych.
5. Dopuszcza się stosowanie wyłącznie licencjonowanego oprogramowania, dopuszczonego do użytkowania przez Administratora Bezpieczeństwa Informacji.

6. Zabrania się instalowania oprogramowania, które jest pirackie, kopiowane lub nielegalnie powielane, jak też programów nie związanych z pracą, gier oraz programów pochodzących z nieautoryzowanych źródeł.
7. Zabronione jest także kopiowanie oprogramowania zainstalowanego na komputerach Urzędu w celu jego instalacji w komputerach domowych, chyba, że jest to specjalnie określone w ramach licencji. Użytkownicy nie mogą na własną rękę instalować żadnego oprogramowania, w szczególności innego niż oficjalnie dopuszczone do użytkownika przez Administratora Bezpieczeństwa Informacji.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

1. Wykaz zbiorów danych osobowych w postaci elektronicznej oraz programy zastosowane do przetwarzania tych danych zostały zawarte w pliku „Dokumentacja IT UM Czersk".
2. Zbiory danych w formie papierowej oraz miejsca ich przechowywania zostały zapisane w „Wykazie zbiorów danych osobowych oraz programy zastosowane do przetwarzania danych osobowych", będącego załącznikiem nr 2 do niniejszej Polityki.
3. 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.

POSTĘPOWANIE W TRAKCIE PRACY NA ZBIORACH DANYCH

LOGIN/ZAREJESTROWANIE PRACOWNIKA

1. Dostęp do systemu informatycznego może uzyskać wyłącznie pracownik zarejestrowany w tym systemie przez Administratora Systemów Informatycznych na wniosek Administratora Bezpieczeństwa Informacji.
2. Dział Kadr Urzędu Miejskiego informuje Administratora Bezpieczeństwa Informacji o każdym nowym pracowniku, a także o ustaniu zatrudnienia lub zaprzestaniu świadczenia usług na podstawie umów cywilnoprawnych.
3. Login użytkownika systemu informatycznego:
   - jest niepowtarzalny,
   - po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielany innej osobie,
   - nie podlega zmianie,
   - jest wpisywany do prowadzonej przez Administratora Bezpieczeństwa Informacji ewidencji użytkowników systemu informatycznego wraz z imieniem i nazwiskiem użytkownika systemu informatycznego.
4. Użytkownicy systemu informatycznego zobowiązani są do zachowania w tajemnicy przed osobami trzecimi ustalonych dla nich loginów.
5. Każdemu nowo przyjętemu pracownikowi jest nadawany login użytkownika nie później niż w momencie rozpoczęcia korzystania z systemów informatycznych.
6. Dla osób czasowo korzystających z zasobów informatycznych – stażyści i praktykanci – tworzone są konta tymczasowe, podlegające identycznym zasadom jak opisano w pkt. 3-5.

HASŁA

7. Hasło użytkownika systemu informatycznego:
   - 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,
   - nie jest zapisywane w systemie, w postaci jawnej,
   - jest zmieniane nie rzadziej, niż co 45 dni,
   - składa się, z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne,
   - jest utrzymywane w tajemnicy, również po upływie jego ważności.

WYREJESTROWANIE PRACOWNIKA, STAŻYSTY LUB PRAKTYKANTA

8. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemów Informatycznych na wniosek Administratora Bezpieczeństwa Informacji.
9. Wyrejestrowanie, o którym mowa w powyżej, może mieć charakter czasowy lub trwały.

10. Wyrejestrowanie następuje poprzez:
    - zablokowanie konta użytkownika systemu informatycznego do czasu ustalenia przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
    - usunięcie danych użytkownika systemu informatycznego z bazy użytkowników systemu informatycznego (wyrejestrowanie trwałe).
11. Przyczyną czasowego wyrejestrowania użytkownika systemu informatycznego z systemu informatycznego jest:
    - nieobecność w pracy trwająca dłużej niż 21 dni kalendarzowych,
    - zawieszenie w pełnieniu obowiązków służbowych,
    - zwolnienie z pełnienia obowiązków służbowych.
12. Przyczyną trwałego wyrejestrowania użytkownika systemu informatycznego z systemu informatycznego jest ustanie zatrudnienia lub zaprzestanie świadczenia usług na podstawie umów cywilnoprawnych, koniec okresu stażu lub praktyki.

ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

13. Rozpoczęcie pracy w systemie informatycznym odbywa się poprzez:
    - przygotowanie stanowiska pracy,
    - włączenie stacji roboczej,
    - wprowadzenie swojego identyfikatora i hasła użytkownika systemu informatycznego.
14. Zakończenie pracy w systemie informatycznym odbywa się poprzez:
    - zamknięcie aplikacji,
    - odłączenie się od zasobów systemowych,
    - zamknięcie systemu operacyjnego,
    - opcjonalnie (w zależności od systemu), wyłączenie stacji roboczej.
15. Czasowe zawieszenie pracy w systemie informatycznym odbywa się poprzez:
    - włączenie w systemie automatycznego wygaszacza ekranu zabezpieczonego hasłem, aktywującego się po 15 minutach od momentu bezczynności stacji roboczej,
    - zabezpieczenie stacji roboczej przez pracownika przed odejściem od stanowiska pracy,
    - lub wylogowanie z systemu informatycznego przez użytkownika systemu - każdorazowe oddalenie się od stacji roboczej musi zostać poprzedzone jej zabezpieczeniem przed niepowołanym dostępem za pomocą sekwencji WINDOWS+ L (Klawisz Windows-L).

ZASADY OGÓLNE

16. 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.

17. Obowiązkiem pracowników, stażystów, praktykantów 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.
18. Używanie przez pracownika komputera przenośnego zawierającego dane osobowe poza budynkiem Urzędu Miejskiego wymaga odnotowania w ewidencji prowadzonej przez Administratora Bezpieczeństwa Informacji.
19. Użytkownik systemu informatycznego odpowiedzialny jest za wszystkie czynności wykonywane przy użyciu identyfikatora i hasła użytkownika systemu informatycznego, którymi się posługuje lub posługiwał.
20. W przypadku powzięcia przez użytkownika systemu informatycznego podejrzenia lub stwierdzenia, że z jego loginem lub hasłem 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 loginu użytkownika systemu informatycznego.
21. Zabrania się użytkownikom systemu informatycznego pracującym w systemie:
    - udostępniania stacji roboczej osobom nie zarejestrowanym w systemie,
    - udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Bezpieczeństwa Informacji,
    - używania nielicencjonowanego oprogramowania,
    - tworzenia kopii danych na nośnikach (CD, DVD, FDD, PEN DRIVE, HDD przenośne i inne) bez zezwolenia Administratora Bezpieczeństwa Informacji,
    - używania nośników w/w do wymiany informacji, bez uprzedniego sprawdzenia programem antywirusowym.
22. Wykaz oprogramowania stosowanego na poszczególnych stanowiskach pracy określa porozumienie zawarte między Administratorem Danych a pracownikiem według wzoru stanowiącego załącznik nr 5.
23. Naruszenie przez użytkownika systemu informatycznego postanowień wskazanych w pkt.16-22, może stanowić podstawę jego odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa.

VIII. BEZPIECZEŃSTWO

BEZPIECZEŃSTWO FIZYCZNE i ŚRODOWISKOWE

1. W celu minimalizacji ryzyk, Urząd stosuje, jako standard, zabezpieczenia fizyczne i środowiskowe wobec informacji i danych oraz elementów infrastruktury teleinformatycznej.
2. Urząd Miejski w Czersku wyposażony jest w elektroniczny system antywłamaniowy z całodobowym monitoringiem sygnału alarmu.
3. Do wszystkich biur i pomieszczeń dostęp jest kontrolowany i nadzorowany. Szczególną ochroną przed dostępem osób trzecich objęte są pomieszczenia, w których znajdują się serwer i węzły sieci oraz pomieszczenia, w których znajdują się zbiory danych. Pomieszczenia te, w czasie nieobecności pracownika powinny być zamknięte.

4. Obszary, w których znajdują szczególnie chronione zasoby i aktywa (np. serwerownia, archiwum) stanowią strefy ograniczonego dostępu, do których dostęp posiadają tylko wyznaczone osoby. Ustalone są zasady dostępu do tych pomieszczeń oraz prowadzona jest ewidencja osób uprawnionych.
5. Osoby trzecie mogą przebywać w tych pomieszczeniach wyłącznie w obecności, co najmniej jednego upoważnionego pracownika. W trakcie prac technicznych wykonywanych przez osoby trzecie, przetwarzanie danych osobowych na wydzielonych stanowiskach jest zabronione, a sprzęt komputerowy musi być wyłączony.
6. Administrator Bezpieczeństwa Informacji prowadzi przegląd procedur i praw dostępu do pomieszczeń przynajmniej raz w roku.
7. Pomieszczenia Urzędu podlegają ochronie polegającej na:
   - zabezpieczaniu przed niepowołanym dostępem i ograniczaniu dostępu osobom niepowołanym,
   - ochronie przeciwpożarowej,
   - kontroli warunków w pomieszczeniach poprzez stosowanie wentylacji i innych stosownych rozwiązań.
   - oraz na stosowaniu innych, uzasadnionych rozwiązań technicznych zabezpieczających pomieszczenie i urządzenia w nim umieszczone przed uszkodzeniem, zniszczeniem i kradzieżą.
8. Administrator Bezpieczeństwa Informacji określa standard zabezpieczeń fizycznych dla pomieszczeń podlegających ochronie fizycznej i dokonuje oceny istniejących zabezpieczeń minimum razy w roku.
9. Każde pomieszczenie chronione posiada wskazaną osobę odpowiedzialną za bezpieczeństwo fizyczne i środowiskowe. Wskazane mogą być wszystkie osoby pracujące w danych pomieszczeniu.
10. Budynek podlega okresowym przeglądom przez uprawnione osoby w zakresie zgodnym z wymaganiami ustawy „Prawo budowlane".

BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA, BEZPIECZEŃSTWO LOGICZNE

11. System informatyczny, ze względu na możliwość połączenia z siecią publiczną, zapewnia środki bezpieczeństwa określone dla wysokiego poziomu bezpieczeństwa.
12. Stosowane są logiczne środki zabezpieczające przed niepowołanym dostępem, utratą lub ujawnieniem danych. Do stosowanych zabezpieczeń należą:
   - loginy użytkownika i hasła w dostępie do stacji roboczych i aplikacji,
   - nadawane prawa dostępu, do odpowiednich obszarów danych, nad którymi nadzór mają: bezpośredni przełożony, Administrator Bezpieczeństwa Informacji, Administrator Systemów Informatycznych,
   - oprogramowanie antywirusowe i wykrywające złośliwe oprogramowanie,
   - firewall'e programowe,
   - zabezpieczanie sieci przed niepowołanym dostępem poprzez zarządzanie domenowe, stałe adresy IP, zarządzanie adresami MAC,
   - ograniczanie i limitowanie przez Administratora Systemów Informatycznych urządzeń dopuszczanych do sieci - brak możliwości dostępu do zasobów i aplikacji Urzędu z komputerów innych niż zaakceptowane przez ABI,
   - zastosowanie stałych adresów IP w sieci,

- ograniczenie uprawnień użytkownikom przez usunięcie uprawnień Administratora na stacjach roboczych i komputerach przenośnych,
- gdy jest to możliwe, ochrona baz danych przed definitywnym usunięciem zapisów,
- zamykanie sesji użytkownika po wykryciu braku aktywności przez 10 minut,
- wykonywanie kopii bezpieczeństwa z ustaloną częstotliwością,
- przechowywanie wykonanych kopii bezpieczeństwa w lokalizacji innej niż pomieszczenia serwerowni, pozwalających na zabezpieczenie przed ich utratą lub zniszczeniem,
- okresowe, nie rzadziej niż raz w roku, sprawdzanie spójności i odtwarzalności kopii bezpieczeństwa.

DOSTĘP DO INTERNETU

13. Dostęp do sieci Internet jest realizowany poprzez:
    - Sieć LAN,
    - poprzez punkt dostępowy WiFi.
14. Dostęp do Internetu dla użytkowników sieci Urzędu jest realizowany poprzez wydzielone łącza telekomunikacyjne. Do przeglądania zasobów Internetu może być wykorzystywana przeglądarka zainstalowana na komputerze.
15. Przeglądanie zasobów Internetu dopuszczalne jest jedynie w związku z bezpośrednim wykonywaniem obowiązków służbowych.
16. Niedopuszczalne jest podłączanie komputera jednocześnie do sieci LAN oraz do Internetu za pomocą sieci radiowych takich jak:
    - WiFi,
    - Sieci mobilne (operatorów komórkowych),
    - Bluetooth.
17. Niedozwolone jest:
    - korzystanie z prywatnej poczty elektronicznej przy użyciu powierzonego przez Urząd sprzętu i oprogramowania. W szczególności zabrania się do korzystania z prywatnej poczty elektronicznej za pomocą przeglądarek,
    - wykorzystywanie zewnętrznych komunikatorów internetowych - np.GaduGadu, Tlen,
    - nie należy otwierać wiadomości e-mail (ani ich załączników) pochodzących od nieznanych nadawców,
    - wszystkie wiadomości e-mail, które nie były oczekiwane, należy traktować z ostrożnością nawet, jeśli znany jest nadawca. W szczególności nie należy otwierać załączników tych wiadomości,
    - nie wolno otwierać plików, które mają podwójne rozszerzenie. (np. wirus.doc.vbs) lub posiadają nieznane dla użytkownika rozszerzenie,
    - w przypadku podejrzeń, co do poprawności funkcjonowania usług sieciowych lub wiarygodności pobranych za pomocą sieci danych (w tym także wiadomości e-mail) należy kontaktować się z Informatykiem Urzędu, przed podjęciem jakichkolwiek działań.

SPOSOBY ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OBCEGO OPROGRAMOWANIA

18. 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.
19. Oprogramowanie, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
20. Niezależnie od ciągłego nadzoru, 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.
21. Do obowiązków Administratora Systemów Informatycznych należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.
22. Zabrania się pracownikom blokowania pracy oprogramowania, o którym mowa w pkt. 18.

OCHRONA DOKUMENTÓW W FORMIE PAPIEROWEJ

23. Dokumenty papierowe o istotnym znaczeniu są odpowiednio chronione. Postępowanie z nimi zostało ustalone i wdrożone - Urząd opracował i stosuje Instrukcję kancelaryjną.
24. Warunki i miejsce przechowywania dokumentów jest określone i przestrzegane. Wszystkie dokumenty Urzędu przechowywane są zgodnie z obowiązującym prawem, ustawami i rozporządzeniami.
25. Dokumentacja finansowo-księgowa musi być przechowywana przez okres, co najmniej 6 lat. Okres przechowywania dokumentów ZUS wynosi 5 lat (zgłoszeniowe) lub 10 lat (rozliczeniowe). Akta osobowe pracowników oraz listy płac należy przechowywać, co najmniej przez 50 lat. Okres przechowywania pozostałych dokumentów zależy od ich osobnych ustaleń, właściwych dla danego rodzaju dokumentu.
26. Dokumenty o wysokim stopniu wrażliwości wrażliwe, np. umowy, akty notarialne, akty własności, inne dokumenty prawne i sądowe przechowywane są w pomieszczeniach o ograniczonym dostępie.
27. Zgodnie z polityką czystego biurka wszystkie dokumenty papierowe muszą być przechowywane w zamkniętych i przeznaczonych do tego miejscach. W szczególności po zakończeniu pracy lub w trakcie przerw, nie wolno pozostawiać dokumentów bez nadzoru.
28. Dokumenty niepodlegające archiwizacji są niszczone w niszczarkach.
29. Kopiowanie dokumentów i dokumentacji, przez pracowników bezpośrednio wynika z realizacji obowiązków służbowych. Kopiowanie dokumentów lub dokumentacji przez osoby nieposiadające uprawnień dostępu do tej dokumentacji lub bez uzasadnienia będzie traktowane jako incydent bezpieczeństwa informacji.
30. Wynoszenie dokumentów poza budynek Urzędu dopuszczalne jest jedynie w przypadkach koniecznych i uzasadnionych trybem postępowania lub zobowiązaniami prawno-administracyjnymi. Nieuzasadnione wynoszenie dokumentów będzie powodowało wyciągnięcie konsekwencji służbowych.

PRZEGLĄDY I AUDYTY UPRAWNIEŃ

31. Administrator Bezpieczeństwa Informacji dokonuje raz w roku przeglądu istniejących uprawnień użytkowników weryfikując istniejące uprawnienia z zapisami w dokumentacji.

32. W ramach przeglądu analizowane są standardowe uprawnienia oraz uprawnienia osób posiadających rozszerzone i niestandardowe uprawnienia. Weryfikowana jest zgodność uprawnień z zasadami podziału obowiązków.
33. Działania te mogą być poddawane niezależnemu audytowi zewnętrznemu.
34. Wyniki przeglądu i audytu są dokumentowane i służą przygotowaniu zmian w zapisach uprawnień.

IX. KONSERWACJE I NAPRAWY

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

   po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.
2. Urządzenia, o których mowa w pkt. 1, przed ich przekazaniem, pozbawia się zapisu danych.
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 zapisu danych osobowych w urządzenia przekazywanym do likwidacji, urządzenie przed przekazaniem uszkadza się w sposób uniemożliwiający odczytanie tych danych.
5. Przeglądy i konserwacje systemu i urządzeń działających w systemie Administrator Systemów Informatycznych dokonuje doraźnie, ale nie rzadziej raz w roku.
6. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemów Informatycznych dokonuje nie rzadziej niż raz na tydzień.
7. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe użytkownik systemu informatycznego przy współudziale Administratora Systemów Informatycznych dokonuje nie rzadziej niż raz na miesiąc.

X. PLANY AWARYJNE I ZAPOBIEGAWCZE, KOPIA BEZPIECZEŃSTWA

1. W przypadku zdarzeń losowych (np. awaria serwera, zalanie pomieszczenia) należy zapewnić uruchomienie systemu w minimalnej konfiguracji udostępniającej zasoby systemu.
2. Kopie bezpieczeństwa tworzy się z następującą częstotliwością:
   - kopie systemu aplikacji dla Administracji Samorządowej - codziennie, oraz dodatkowo jedna kopia z całego tygodnia,
   - kopie pozostałych systemów informatycznych - nie rzadziej niż raz w tygodniu.
3. Kopie dzienne kasowane są po tygodniu. Kopie tygodniowe kasowane są po miesiącu.
4. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu. Niszczenia kopii zapasowych na nośnikach magnetycznych dokonuje Administrator Systemów Informatycznych.
5. Kopie tworzone są automatycznie w czasie gdy pracownicy nie korzystają z danych na serwerze. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
6. Kopie te wykonuje się na nośniku magnetycznym, które to nośniki przechowuje się w sejfie umieszczonym w pomieszczeniu innym, niż dane osobowe przetwarzane na bieżąco. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

7. Kopie bezpieczeństwa podlegają takiej samej ochronie jak serwery zawierające dane osobowe.
8. Administrator Systemów Informatycznych dokonuje okresowych przeglądów kopii awaryjnych i ocenia ich przydatność do odtworzenia zasobów systemu informatycznego w przypadku jego awarii.
9. 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.
10. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
11. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych osobowych należy wymontować go z komputera i fizycznie zniszczyć.
12. Likwidacji wydruków dokonuje się przy użyciu przeznaczonych do tego celu urządzeń (np. niszczarek).

XI. POSTĘPOWANIE W SYTUACJI NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

ZAŁOŻENIA OGÓLNE

1. Działania podejmowane przez Urząd mają na celu przewidywanie, eliminowanie i wykrywanie naruszeń bezpieczeństwa informacji (incydentów).
2. Wszyscy pracownicy Urzędu mają obowiązek informowania Administratora Bezpieczeństwa Informacji lub swojego przełożonego o zauważonych incydentach bezpieczeństwa.
3. Wystąpienie incydentu jest analizowane przez Administratora Bezpieczeństwa Informacji wraz z zespołem technicznym i w uzasadnionych przypadkach ekspertami zewnętrznymi w celu wprowadzenia zmian i usprawnień w systemie bezpieczeństwa informacji.
4. Administratora Bezpieczeństwa Informacji, wspólnie z administratorem sieci planuje działania mające na celu minimalizację ryzyka wystąpienia zagrożeń poprzez planowanie zabezpieczeń i procedur, wdrażanie nowych rozwiązań oraz analizę wykrytych incydentów.
5. Wszystkie wykryte lub prawdopodobne przypadki naruszenia bezpieczeństwa informacji są zgłaszane do Administratora Bezpieczeństwa Informacji, który analizuje przypadek i sugeruje podjęcie działań minimalizujących skutki incydentu oraz działania korygujące, tak aby zapobiegać podobnym incydentom w przyszłości.
6. Administrator sieci stale monitoruje poziom bezpieczeństwa oraz pojawiające się zagrożenia.
7. Każdy pracownik Urzędu Miejskiego, który stwierdził:
   - naruszenie bezpieczeństwa systemu informatycznego,
   - naruszenie technicznego stanu urządzeń służących do przetwarzania danych osobowych,
   - naruszenie zawartości zbioru danych osobowych,
   - ujawnienie metod pracy lub sposobów działania programu osobom trzecim,
   - zmianę jakości transmisji danych w sieci telekomunikacyjnej mogącą wskazywać na naruszenie zabezpieczenia tych danych,
   - zaistnienie innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, itp.),

   obowiązany jest niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

INCYDENTY BEZPIECZEŃSTWA INFORMACJI

8. Przez incydent naruszenia bezpieczeństwa informacji rozumie się zdarzenie, w wyniku którego doszło do ujawnienia lub utraty albo zwiększenia ryzyka ujawnienia lub utraty informacji, która nie jest uznana za informację publiczną.
9. Źródłem takich informacji o incydentach mogą być:
   - obserwacje i zgłoszenia pracowników Urzędu,
   - obserwacje Administratorów,
   - sygnały z oprogramowania, np. antywirusy, firewall'e.
   - audyty bezpieczeństwa.
10. Jako potencjalne zdarzenia mające wpływ na bezpieczeństwo zalicza się np. następujące zdarzenia:
   - wykrycie wirusa lub złośliwego oprogramowania,
   - wykrycie nieautoryzowanego dostępu lub próby nieautoryzowanego dostępu do systemów informatycznych,
   - wykrycie w sieci LAN nieautoryzowanych urządzeń,
   - próby uruchamiania aplikacji przez użytkownika nie posiadającego praw dostępu,
   - podłączanie do sieci nieautoryzowanych urządzeń,
   - wykrycie urządzeń posiadających inną niż opisana w dokumentacji konfigurację,
   - błędy administratorów,
   - awarie urządzeń i oprogramowania skutkujące zwiększonym zagrożeniem,
   - niestandardowe zachowanie osób mających dostęp do systemów,
   - ujawnienie lub prawdopodobne ujawnienie hasła użytkownika,
   - nieautoryzowane próby dostępu do systemów,
   - próby łamania haseł,
   - próby dostępu spoza sieci z nieautoryzowanych urządzeń,
   - przebywanie w pomieszczeniach o ograniczonym dostępie osób nie posiadających upoważnienia,
   - utrata, zagubienie lub uprawdopodobnienie skopiowania danych lub informacji będących tajemnicą lub istotną i chronioną z innego powodu,
   - próby nieuzasadnionego i niekontrolowanego odtwarzania kopii zapasowych (poza koniecznym odtwarzaniem takich kopii w przypadkach awarii lub w celu weryfikacji poprawności kopii),
   - nieuzasadnione i nieuprawnione kopiowania danych,
   - udostępnianie informacji na temat sposobu zabezpieczenia lub ochrony systemu informatycznego Urzędu osobom do tego nieupoważnionym,
   - samodzielne instalowanie jakiegokolwiek oprogramowania,
   - dokonywanie nieuprawnionych modyfikacji konfiguracji wykorzystywanego sprzętu lub oprogramowania,
   - podłączanie do systemu prywatnych nośników danych (np. pamięci USB, odtwarzaczy mp3 itp.),

- nieuprawnione przenoszenie danych na wszelkiego rodzaju nośniki (papierowe, magnetyczne, elektroniczne, etc.).
- nieupoważnione kopiowanie dokumentacji.

11. Także inne przypadki, nie wymienione powyżej mogą być klasyfikowane jako naruszenie bezpieczeństwa informacji.
12. Incydenty naruszenia bezpieczeństwa informacji są klasyfikowane według stopnia naruszenia PID - **P**oufność, **I**ntegralność, **D**ostępność.
    a. incydent o niskiej szkodliwości – na skutek zdarzenia nastąpiło zagrożenie danych, ale zdarzenie nie wymaga podjęcia natychmiastowych działań, lub działania takie zostały przewidziane wcześniej, są opisane, ale nie wymagają działań ze strony Administratorów.
    b. incydent o wysokiej szkodliwości – na skutek zdarzenia nastąpiło znaczne zwiększenie ryzyka PID. Zdarzenie takie nie zostało wcześniej opisane w szczegółowych instrukcjach i wymaga działań ze strony Administratora i ABI.
    c. incydent krytyczny – na skutek zdarzenia zostały ujawnione lub utracone informacje lub dane chronione. Wymagane są bezzwłoczne i natychmiastowe działania Administratorów.
13. W przypadku zaistnienia incydentu o wysokiej szkodliwości lub krytycznego pracownik jest zobowiązany do zgłoszenia tej sytuacji Administratora Bezpieczeństwa Informacji. Do czasu przybycia Administratora Bezpieczeństwa Informacji na miejsce naruszenia ochrony danych osobowych, należy:
    - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie w miarę możliwości ustalić przyczyny lub sprawców,
    - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
    - zaniechać (o ile to możliwe) dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
    - podjąć inne działania stosownie do objawów i komunikatów towarzyszących naruszeniu w szczególności określone w instrukcjach technicznych,
    - podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
    - zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
    - udokumentować wstępnie zaistniałe naruszenie,
    - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia.
14. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator Bezpieczeństwa Informacji w szczególności:
    - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
    - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
    - rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych i Administratora Systemów Informatycznych.

15. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia sporządzając raport wg wzoru stanowiącego załącznik nr 3, który powinien zawierać w szczególności:
    - wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
    - określenie czasu i miejsca naruszenia i powiadomienia,
    - określenie okoliczności towarzyszących i rodzaju naruszenia,
    - wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
    - wstępną ocenę przyczyn wystąpienia naruszenia,
    - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
16. W przypadkach incydentów naruszenia danych osobowych, Administrator Bezpieczeństwa Informacji zobowiązuje Administratora Systemów Informatycznych do sporządzenia raportu, którego treść stanowi załącznik nr 3 do niniejszego dokumentu. Raport, ten niezwłocznie przekazuje Administratorowi Danych.
17. Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych propozycję postępowania naprawczego oraz termin wznowienia przetwarzania danych osobowych.

XII. LISTA ZAŁĄCZNIKÓW

Załącznik nr 1 - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Załącznik nr 2 - wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania danych osobowych.

Załącznik nr 3 - Raport z naruszenia bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Czersku.

Załącznik nr 4 - Wykaz pracowników zatrudnionych przy przetwarzaniu danych osobowych, którzy zostali zapoznani z Polityką Bezpieczeństwa w Urzędzie Miejskim w Czersku.

Załącznik nr 5 - Wykaz stażystów i praktykantów zatrudnionych przy przetwarzaniu danych osobowych, którzy zostali zapoznani z Polityką Bezpieczeństwa w Urzędzie miejskim w Czersku.

Załącznik nr 6 - Porozumienie z pracownikiem.

Załącznik nr 7 - Porozumienie z stażystą lub praktykantem.

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

Budynek / Skrzydło	Nr pomieszczenia	Komórka organizacyjna

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

Wykaz stażystów i praktykantów 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 6
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 _____ 20__ 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

Załącznik nr 7
do polityki ochrony danych przetwarzanych
w systemach informatycznych Urzędu
Miejskiego w Czersku

WZÓR

Porozumienie z stażystą lub praktykantem

Niniejsze porozumienie (zwane dalej „Porozumieniem") zostało zawarte w dniu _____ 20__ r. w _____ pomiędzy:

Urzędem Miejskim w Czersku, reprezentowanym przez _____, zwanym dalej „Pracodawcą"

oraz

Panią/Panem _____, zamieszkałą/ym w _____ przy ul. _____ , zwaną/ym dalej „stażystą lub praktykantem".

Wstęp:

(A) Stażysta lub Praktykant zatrudniony jest przez Pracodawcę na podstawie umowy stażowej lub umowy o praktykę zawartej w dniu _____ r.

(B) Pracodawca wyposażył stanowisko pracy Stażysty lub Praktykanta w oprogramowanie komputerowe _____, na używanie którego licencję nabył od _____ („Oprogramowanie").

Odpowiednie przepisy regulują w sposób szczegółowy zasady korzystania z Oprogramowania.

(C) Stażysta lub Praktykant korzysta z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych.

1. Pracodawca i Stażysta lub Praktykant uzgadniają, że do podstawowych obowiązków Stażysty lub Praktykanta 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. Stażysta lub Praktykant 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 Stażysta lub Praktykant uzgadniają, że naruszenie przez Stażystę lub Praktykanta 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 staż lub praktykę, łączącej Pracodawcę z Stażystą lub Praktykantem, lub rozwiązanie przez Pracodawcę tejże umowy o staż lub praktykę bez wypowiedzenia, z winy stażysty lub praktykanta, 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