ZARZĄDZENIE NR 89/09
BURMISTRZA BIAŁEGO BORU
z dnia 01 września 2009 r.

w sprawie: wprowadzenia dokumentacji opisującej podstawowe zasady bezpieczeństwa systemów informatycznych zwanej „polityką bezpieczeństwa".

Na podstawie art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity: Dz. U. z 2001 nr 142, poz 1591 z późn. zm.) art 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (tekst jednolity: Dz.U. z 2004 r. Nr 100, poz. 1024) zarządzam co następuje:

§ 1
Ustala się Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Białym Borze, zwaną dalej „Polityką bezpieczeństwa", stanowiącą załącznik do niniejszego zarządzenia.

§ 2
„Polityka bezpieczeństwa", określa zespół zasad i działań podejmowanych w celu bezpiecznego korzystania z systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Białym Borze, procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń oraz prawa i obowiązki użytkowników systemu informatycznego.

§ 3
Wszyscy pracownicy Urzędu Miejskiego korzystający z systemu informatycznego i przetwarzający dane osobowe zobowiązani są zapoznać się z polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe oraz aktualnymi przepisami prawnymi w zakresie ochrony danych osobowych i podpisać stosowne oświadczenie.

§ 4
Wykazy osób potwierdzających fakt zapoznania się z wyżej wymienioną problematyką należy przekazać wraz z podpisanym oświadczeniem Administratorowi Bezpieczeństwa Informacji.

§ 5
Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Franciszek Lech Kwaśniewski

Załącznik
do Zarządzenia nr 89/09
Burmistrza Białego Boru
Z dnia 01.09.2009 r.

PODSTAWOWE ZASADY BEZPIECZEŃSTWA SYSTEMÓW **INFORMATYCZNYCH**

URZĘDU MIEJSKIEGO W BIAŁYM BORZE

„POLITYKA BEZPIECZEŃSTWA"

opracowanie: 2009 rok

Cel opracowania polityki bezpieczeństwa

Celem stosowania podstawowych zasad bezpieczeństwa systemów informatycznych jest wskazanie działań, jakie należy wykonywać i stosować oraz ustanowienie zasad i reguł postępowania, aby zagwarantować ochronę danych osobowych i innych danych informatycznych przetwarzanych w Urzędzie Miejskim.

Zastosowanie się do zasad podstawowej polityki bezpieczeństwa ma zapewnić:

- niedopuszczenie do utraty, uszkodzenia lub zniszczenia danych,
- niedopuszczenie do utraty integralności danych,
- niedopuszczenie do ujawnienia danych osobom nieuprawnionym.

Zagrożenia

Podstawowymi zidentyfikowanymi zagrożeniami systemów informatycznych są:

- kradzież danych,
- kradzież nośników danych – dysków twardych, dysków wymiennych, komputerów,
- udostępnienie danych poprzez przekopiowanie danych, poprzez osoby nieuprawnione,
- udostępnienie danych poprzez nieumyślne lub celowe wysyłanie danych osobowych poprzez internet, bez zachowania odpowiednich zabezpieczeń,
- udostępnienie danych poprzez wgląd w dane przez osoby nieuprawnione (np. wgląd w ekran, monitor, udostępnienie stanowiska komputerowego osobie nieuprawnionej),
- udostępnienie danych poprzez nieumyślne lub celowe udostępnienie dysków, katalogów zawierających dane,
- utrata danych w skutek awarii nośników danych i innych awarii sprzętowych,
- utrata danych w skutek awarii zasilania,
- utrata danych w skutek działania wirusów,
- utrata danych w skutek braku kontroli poprawności działania baz danych (utrata spójności bazy, uszkodzenia indeksów bazy),
- kradzież lub udostępnienie kluczy prywatnych, certyfikatów, tokenów, kart chip itp.,
- udostępnienie identyfikatorów (loginów) i/lub haseł,
- utrata danych w skutek błędu programu użytkowego,
- niezamierzona zmiana danych w skutek błędu programu komputerowego,
- niezamierzona zmiana danych w skutek błędu popełnionego przez użytkownika,
- utrata danych w skutek żywiołu.

Uświadomienie ewentualnych skutków wywołanych zagrożeniami.

W praktyce najczęstszymi (obok wielu innych, jak wyżej) przyczynami utraty danych lub ich spójności jest pozostawienie lub udostępnienie uruchomionego stanowiska z zalogowanymi (spersonalizowanymi aplikacjami do pracy w kontekście uprawnionej osoby) innym, często nieuprawnionym osobom lub całkowicie bez kontroli.

Ponieważ za pomocą systemów informatycznych realizuje się coraz więcej i coraz bardziej odpowiedzialne (również finansowe) zadania, użytkownik powinien mieć

świadomość, że pozostawiając spersonalizowany uruchomiony system bez kontroli lub do dyspozycji innych osób może narazić się na ryzyko.
Nieautoryzowane i nie kontrolowane czynności podczas jego nieobecności bądź braku możliwości kontroli tych czynności na stanowisku są rejestrowane przez systemy jako wykonane przez właściwego użytkownika i to użytkownik pozostawiający/udostępniający stanowisko i aplikację ponosi konsekwencje z tym związane.
Innym, niebagatelnym, często pojawiającym się ostatnio zagrożeniem jest zainfekowanie komputerów przy użyciu pendrive (dysków przenośnych USB), pochodzących spoza urzędu lub używanych również poza nim, przez samego użytkownika lub poprzez udostępnienie swojego komputera w celu podłączenia tego typu nośników danych innym osobom.
Używanie tego typu dysków w komputerach nie mających odpowiednich zabezpieczeń poza urzędem, a następnie korzystanie z nich w urzędzie, niesie za sobą ogromne zagrożenie nieświadomego przeniesienia np. wirusów i innego szkodliwego oprogramowania, a w konsekwencji ewentualnością całkowitej utraty danych (często wielu lat pracy) lub zniszczenie sprzętu.

Przeciwdziałanie.

1. Przetwarzanie danych w systemach informatycznych powinno odbywać się wyłącznie w budynku, pomieszczeniach i komputerach wyznaczonych do tego celu.
2. Do przetwarzania danych w systemie informatycznym mogą być dopuszczone wyłącznie osoby upoważnione przez administratorów danych i tylko w wyznaczonym zakresie tych danych i systemów.
3. Administratorów danych i administratorów systemów informatycznych wyznacza Burmistrz lub uprawniona przez niego do tego osoba w sposób ustny lub pisemny.
4. Identyfikatory, loginy, hasła i uprawnienia w systemach informatycznych nadają administratorzy.
5. Niedopuszczalnym jest samodzielna nieuprawniona próba zmiany lub zmiana przez użytkowników nie będących administratorami, danych pozwalających uzyskiwać dostęp do zasobów systemowych innym użytkownikom, a w szczególności samym administratorom.
6. Po ustaniu zatrudnienia lub po odebraniu uprawnienia osobie przetwarzającej dane administratorzy powinni blokować użytkownika (identyfikator) w systemie informatycznym, aby uniemożliwić zalogowanie do systemu informatycznego.
7. Jeżeli złożoność systemu informatycznego wyklucza możliwość przydzielenia różnych identyfikatorów kilku użytkownikom, należy zadbać o zabezpieczenie/hasło na wyższym poziomie.
8. Zalogowanie do systemu informatycznego przetwarzającego dane następuje po wprowadzeniu identyfikatora i hasła. Wyjątek stanowić może system, w którym dane przetwarza tylko jedna osoba, wówczas dostęp możliwy jest po wprowadzeniu hasła.
9. Zarówno identyfikatorów, jak i haseł indywidualnych nie wolno przekazywać innym osobom, a w szczególności osobom

nieuprawnionym do przetwarzania danych. Obowiązek ten istnieje również po ustaniu zatrudnienia.

10. Hasła należy zmieniać okresowo.
11. Należy wykonywać kopie zapasowe danych lub zadbać o ich wykonanie i zabezpieczenie.
12. Użytkownik winien sam zadbać o archiwizację danych wytworzonych przez siebie typu (zdjęcia, pisma, pocztę wychodzącą i przychodzącą, tabele, inne)
13. Administrator archiwizuje dane systemów esod, zsi, selwin, fkp, oraz innych programów będących zainstalowanych na serwerze do użytku ogólnego lub częściowego.
14. Jeżeli użytkownik nie ma możliwości samodzielnie zarchiwizować swoich danych/dokumentów (np. nie posiada nagrywarki lub system nie umożliwia tego użytkownikowi), ze względu na coraz większą ilość danych i systemów komputerowych wykorzystywanych w urzędzie, na użytkowniku spoczywa obowiązek dopilnowania okresowego wykonania kopi bezpieczeństwa swojego systemu lub swoich danych przez administratorów.
15. Użytkownik konkretnego systemu informatycznego ma najlepszą orientację w jakim okresie lub czasie wprowadził, lub zmienił znaczne ilości danych w swoim systemie, dlatego powinien zadbać aby w najbliższym czasie wykonana została kopia bezpieczeństwa tych danych. Jeżeli nie jest w stanie zrobić tego sam powinien zgłosić się do administratorów.
16. Użytkownik powinien również dopilnować wykonania kopi bezpieczeństwa danych przed wykonaniem rzadszych i niestandardowych procedur w systemie informatycznym, np. zamknięciem lub otwarciem roku w systemie, aktualizacjami systemu i innymi czynnościami niosącymi za sobą ryzyko nieodwracalnych, niepożądanych zmian w systemie informatycznym.
17. Jeżeli użytkownik uzna, że kopia systemu informatycznego, w którym pracuje nie była dawno wykonywana, należy zgłosić to administratorom.
18. Każdy użytkownik zobowiązany jest do przeprowadzania kontroli antywirusowej wszystkich używanych przez siebie nośników danych lub zadbanie aby taka kontrola została przeprowadzona.
19. Wymienne nośniki danych (np. pendrive) mogą zostać podłączone wyłącznie wtedy, gdy zachodzi taka konieczność. Jest wskazane aby odbyło się to po uzgodnieniu z administratorami. Należy wówczas bezwzględnie i każdorazowo kontrolować nośnik aktualnym programem antywirusowym.
20. W przypadku, gdy na stanowisku komputerowym nie jest zainstalowany program antywirusowy lub nie jest aktualny, nie należy wkładać ani podłączać wymiennych nośników danych (dyskietek, płyt, pendrive, itp.).
21. W przypadku, gdy na stanowisku komputerowym nie jest zainstalowany program antywirusowy lub nie jest aktualny, nie należy korzystać z internetu.
22. W przypadku, gdy subskrypcja na aktualizację oprogramowania antywirusowego dobiega lub dobiegła końca, należy powiadomić

administratorów. W takim przypadku należy odnowić subskrypcję lub dokonać zakupu i instalacji nowego oprogramowania antywirusowego.

23. W przypadku, gdy system operacyjny lub oprogramowanie zabezpieczające (program antywirusowy i/lub zapora) sygnalizuje o jakichkolwiek błędach zabezpieczeń, należy fakt ten zgłosić administratorom.
24. Należy wykonywać przeglądy i konserwacje systemów.
25. Użytkownik powinien mieć świadomość korzyści ale i zagrożeń jakie niesie ze sobą korzystanie z internetu, komunikatorów internetowych (np. gg, skype) oraz poczty internetowej.
26. W przypadku stwierdzenia awarii sprzętowych, należy powziąć szczególne środki ostrożności tzn. niezwłocznie zapisać dane, ograniczyć lub całkowicie zaprzestać pracy, wyłączyć komputer i powiadomić administratorów.
27. W pomieszczeniach, gdzie znajdują się osoby postronne, monitory należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.
28. Bez wiedzy administratorów nie należy samodzielnie dokonywać modyfikacji sprzętowych lub systemowych.
29. Bez wiedzy administratorów nie należy modyfikować udostępnionych haseł, w szczególności innym użytkownikom, a jeżeli system wymusza to automatycznie należy poinformować o zmianie administratorów.
30. Użytkownik/pracownik zobligowany jest dopilnować aby w obrębie jego stanowiska pracy konfigurację, przełączanie, przenoszenie i inne czynności techniczne dotyczące sprzętu komputerowego, okablowania i sprzętu peryferyjnego wykonywali wyłącznie administratorzy informatycy lub firma informatyczna (serwis). Tego typu czynności nie może wykonywać osoba spoza urzędu bez wcześniejszego uzgodnienia z administratorami.
31. Użytkownik powinien zdeponować wszelkiego rodzaju hasła (do systemu, platform) w zapieczętowanej kopercie u Administratora i Sekretarza Gminy.
32. Klucze prywatne, a także tokeny, karty magnetyczne i chipowe, należy chronić przed osobami nieuprawnionymi.
33. Każdy użytkownik powinien zadbać aby na jego stanowisku komputerowym zostało ustawione przez administratorów hasło startowe (bios) i aby było ono aktywne tzn. istniała konieczność jego poprawnego wpisania aby uruchomić komputer.
34. Pracownik opuszczający stanowisko pracy z komputerem nawet na chwilę, zobowiązany jest wylogować się z systemu informatycznego służącego do przetwarzania danych. Powinien również dodatkowo wylogować się z systemu operacyjnego.
35. W godzinach pracy – w czasie nieobecności pracowników w biurze, pomieszczenia, w którym przetwarzane są dane należy zamykać na klucz (po uprzednim wylogowaniu z systemów).
36. Po zakończeniu pracy komputer należy wyłączyć.
37. Po godzinach pracy ostatnia osoba opuszczająca obiekt, w którym przetwarzane są dane osobowe zobowiązana jest zabezpieczyć pomieszczenia i budynek w sposób uniemożliwiający wejście osób nieuprawnionych.

38. Przechowywanie prywatnych danych np. fotografii, filmów itp. ma znaczny wpływ na pojemność dysków systemowych i znaczne wydłużenie czasu wszelkich czynności serwisowych dlatego nie powinno mieć miejsca.

W sytuacjach, gdy:

- zachodzi konieczność podjęcia istotnej decyzji dotyczącej zabezpieczeń systemu informatycznego,
- zachodzi konieczność rozbudowy systemów informatycznych, infrastruktury informatycznej,
- nastąpi podejrzenie złamania zabezpieczeń systemu informatycznego,
- zachodzi konieczność dokonania zmian sprzętowych lub systemowych,
- nastąpiła awaria sprzętu,

należy zasięgnąć rady i pomocy administratorów/informatyków lub firmy informatycznej (serwisu).
W wyjątkowych sytuacjach np. serwisowych mając na uwadze bezpieczeństwo, naprawę, odzyskanie, ochronę danych lub w celach testowych systemów, administratorzy mogą wyjątkowo (chwilowo) odstąpić od niektórych zasad Polityki Bezpieczeństwa zachowując jednak ogólne zasady bezpieczeństwa danych informatycznych.

Uwagi końcowe

W sprawach nieuregulowanych niniejszą Polityką Bezpieczeństwa, zastosowanie mają przepisy wynikające z ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych. Wszyscy pracownicy zobowiązani są do przestrzegania zasad bezpieczeństwa opisanych w niniejszej Polityce Bezpieczeństwa.

Definicje

(większość definicji wg. wikipedii – wolnej encyklopedii internetowej) Definicje użyte w niniejszym opracowaniu:

administrator - (potocznie admin) – informatyk zajmujący się zarządzaniem całością lub wydzieloną częścią systemu informatycznego, odpowiadający za jego sprawne działanie. Wyróżnia się administratorów: systemów operacyjnych, baz danych, serwerów, sieci, stron internetowych.

administrator bezpieczeństwa informacji – osoba wyznaczona przez administratora danych nadzorująca przestrzeganie zasad ochrony, o których mowa w ust. 1 ustawy o ochronie danych osobowych.

administrator danych – organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydująca o celach i środkach przetwarzania danych osobowych.

baza danych - zbiór danych zapisanych w ściśle określony sposób w strukturach odpowiadających założonemu modelowi danych. W potocznym ujęciu obejmuje dane oraz program komputerowy wyspecjalizowany do gromadzenia i przetwarzania tych danych. Program taki (często pakiet programów) nazywany jest "Systemem zarządzania bazą danych" (ang. DataBase Management System, DBMS).

BIOS – (ang. Basic Input/Output System – podstawowe procedury wejścia/wyjścia) to zapisany w pamięci stałej, inny dla każdego typu płyty głównej komputera, zestaw podstawowych procedur pośredniczących pomiędzy systemem operacyjnym, a sprzętem. Program konfiguracyjny BIOS-a to BIOS setup, który umożliwia zabezpieczenie komputera już od momentu jegowłączenia.

dane - (ang. data; z łac. datum - to, co jest dane) – w informatyce zbiory liczb i tekstów o różnych formach. Są one używane przez komputery do obliczeń oraz są prezentowane, czy też przetwarzane cyfrowo. Takie tematyczne zbiory informacji są nazwane bazami danych. Mogą być olbrzymie, połączone w sieć poprzez internet czy intranet i posiadać różne systemy zabezpieczeń chroniące je przed nieupoważnionymi osobami. W najbardziej ogólnym systemowym sensie dane są zdefiniowane jako "to wszystko co jest/może być przetwarzane umysłowo lub komputerowo".

firewall/zapora – narzędzie programowe lub sprzętowe, którego zadaniem jest kontrola pakietów przesyłanych z sieci LAN do sieci publicznej i odwrotnie.

hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedyne osobie lub osobom uprawnionym do pracy w systemie informatycznym.

identyfikator użytkownika/login – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym. Słowo login wywodzi się z języka angielskiego od skrótu log in, określającego zalogowanie się do systemu. Procesem odwrotnym do logowania jest tzw. wylogowanie (ang. log out).

Integralność danych – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

interfejs - oprogramowanie pozwalające na interakcję między aplikacjami i użytkownikiem.

internet – sieć publiczna, zewnętrzna, ogólnoświatowa sieć komputerowa.

karta chip - karta elektroniczna, karta chipowa (ang. smart card) – uniwersalny nośnik danych w postaci karty wykonanej z plastiku z umieszczonym na niej (lub wewnątrz niej) jednym lub kilkoma układami scalonymi (chip), które pozwalają na ochronę procesu logowania użytkownika, kontrolę dostępu i zawartych na niej danych. Może być odczytywana za pomocą urządzeń automatycznych, np. przy

zawieraniu i rozliczaniu transakcji finansowych oraz w kasach cyfrowych. Karty elektroniczne mają rozmiar i wygląd zbliżony do tradycyjnych kart kredytowych z paskiem magnetycznym. Często posiadają również taki pasek i mogą być odczytywane w urządzeniach nie obsługujących kart elektronicznych.

klucz prywatny to w kryptografii asymetrycznej (przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem) klucz służący do wykonywania zastrzeżonej czynności, którego rozpowszechnienie zagraża bezpieczeństwu systemu. Czynności te to najczęściej: odszyfrowywanie (klucz publiczny szyfruje), podpisywanie (klucz publiczny weryfikuje podpisy).

LAN/sieć lokalna/eternet – sieć lokalna (ang. Local Area Network stąd używany także w języku polskim skrót LAN) (wewnętrzna sieć) – najmniej rozległa postać sieci komputerowej, zazwyczaj ogranicza się do jednego budynku lub kilku pobliskich budynków.

logowanie - rodzaj uwierzytelnienia i autoryzacji użytkownika polegający na podawaniu loginu i hasła w celu wejścia do określonego systemu informatycznego lub otrzymanie w nim określonych uprawnień.

nośnik danych – przedmiot (ciało fizyczne), na którym możliwe jest fizyczne zapisanie danego rodzaju informacji, i z którego możliwe jest późniejsze odczytanie (odtworzenie) tej informacji. Pod pojęciem nośnik danych najczęściej rozumie się przedmioty ściśle związane z komputerami: dysk, płyta, dyskietka, pendrive lub inne urządzenia, na którym można zapisać dane w formie elektronicznej.

Nazwa nośnika Nazwa urządzenia

karta dziurkowana czytnik kart dziurkowanych i dziurkarka kart dziurkowanych taśma dziurkowana czytnik taśmy dziurkowanej i dziurkarka taśmy dziurkowanej taśma magnetyczna magnetofon, streamer, pamięć taśmowa bęben magnetyczny pamięć bębnowa, dyskietka magnetyczna 3,5" - DD, HD, 2HD stacja dyskietek FDD 1,44 MB, 2,88 MB, 720 kB do 2,88 MB, dyskietka magnetyczna 5,25" - 360 kB do 1,2MB, stacja dysków FDD 1,2 MB, dyskietka magnetyczna 8", dyskietka magnetyczna typu ZIP nap d ZIP 100, 250 lub 750 MB dysk magnetyczny 10 MB do kilku TB dysk twardy HDD dyski CD-Audio czytnik CD-ROM, urządzenia audio, urządzenia do zapisu CD-RW, dyski optyczne CD do 870 MB czytnik CD-ROM, urządzenia do zapisu CD-RW, dyski optyczne DVD - 4,7 GB - 18 GB czytnik DVD, dyski optyczne Blu- ray (BD) - 25 GB - 200 GB czytnik BD, Karty pamięci - 8 MB - 64 GB czytnik kart Pendrive - 8 MB - 64 GB Komputer wyposażony w złącze USB (ew. przenośny dysk OnTheGo)

p2p/peer to peer (od ang. peer-to-peer – równy z równym) – model komunikacji w sieci komputerowej, który gwarantuje obydwu stronom równorzędne prawa (w przeciwieństwie do modelu klient-serwer).

pendrive - Pamięć USB (znana także pod nazwami: PenDrive, USB Flash Drive, Flash Disk, FlashDrive, Finger Disk, Massive Storage Device, Flash Memory Stick Pen Drive, USB-Stick) - urządzenie przenośne zawierające pamięć nieulotną typu Flash EEPROM, zaprojektowane do współpracy z większością komputerów poprzez port USB i używane do przenoszenia danych (zapisywanych w plikach) między komputerami. Spopularyzowana również w Polsce nazwa marki urządzenia PenDrive (ang. pen, "pióro" + drive, "nap d") odnośnie wszystkich typów pamięci USB rozpowszechniła się najprawdopodobniej ze względu na skojarzenia - pochodzi od wyglądu przypominającego najczęściej krótki długopis z zaślepką (na wtyk USB).

poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

program komputerowy (ang. computer program) - sekwencja symboli opisująca obliczenia, zgodnie z pewnymi regułami zwanymi językiem programowania[1]. Program jest zazwyczaj wykonywany przez komputer (np. wyświetlenie strony internetowej), czasami bezpośrednio, jeśli wyrażony jest w języku zrozumiałym dla danej maszyny lub pośrednio, gdy jest interpretowany przez inny program (interpreter). Program może być ciągiem instrukcji opisujących modyfikacje stanu maszyny, ale może również opisywać obliczenia w inny sposób (np. rachunek lambda). Programy komputerowe można zaklasyfikować według ich zastosować. Wyróżnia się, zatem aplikacje użytkowe, systemy operacyjne, gry wideo, kompilatory i inne. Programy wbudowane wewnątrz urządzeń określa się jako firmware. Formalne wyrażenie metody obliczeniowej w postaci języka zrozumiałego dla człowieka nazywane jest kodem źródłowym, podczas gdy program wyrażony w postaci zrozumiałej dla maszyny (to jest za pomocą ciągu liczb, a bardziej precyzyjnie zer i jedynek) nazywany jest kodem maszynowym bądź postacią binarną (wykonywalną).

przetwarzanie danych - termin prawniczy, który w prawie polskim zostać zdefiniowany w ustawie dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) (ustawodawca posłużył się określeniem przetwarzanie danych). Przetwarzanie oznacza jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

sieć publiczna – sieć publiczna w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne.

sieć telekomunikacyjna – sieć telekomunikacyjna w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.).

system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

token - generator kodów jednorazowych – urządzenie elektroniczne służące do uwierzytelniania transakcji internetowych, najczęściej bankowych. Jego działanie polega na generowaniu ciągów cyfr za pomocą funkcji jednokierunkowej wykorzystującej dwa parametry - jeden stały dla konkretnego egzemplarza urządzenia, drugi zmienny - wprowadzany za pomocą klawiatury, wczytywany z ekranu monitora, bądź generowany na podstawie czasu. Niektóre modele tokenów są zabezpieczone przed użyciem za pomocą systemu haseł.

USB - (ang. Universal Serial Bus – uniwersalna magistrala szeregowa) – rodzaj sprzętowego portu komunikacyjnego komputerów, zastępującego stare porty szeregowe i porty równoległe. Zostać opracowany przez firmy Microsoft, Intel, Compaq, IBM i DEC. Port USB jest uniwersalny w tym sensie, że można go wykorzystać do podłączenia do komputera wielu różnych urządzeń (np.: kamery wideo, aparatu fotograficznego, telefonu komórkowego, modemu, skanera, klawiatury, przenośnej pamięci, nośników danych itp.).

ustawa o ochronie danych osobowych – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883 z pó.n zm.).

usuwanie danych – to czynność_ usuwania zawartości nośnika komputerowego w sposób, który utrudnia lub uniemożliwia ich późniejsze odtworzenie, zniszczenie danych.
uwierzytelnienie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
Użytkownik (w kontekście informatycznym) - jest to osoba lub inny system korzystający z systemu komputerowego. Użytkownicy uzyskują dostęp do systemów przez interfejs użytkownika, a sam proces identyfikacji jest nazywany Logowaniem (od angielskiego logging in). Użytkownicy są powszechnie charakteryzowani jako osoby, które korzystają z systemu bez pełnej wiedzy technicznej, pozwalającej na zrozumienie jego sposobu funkcjonowania.
wylogowanie - proces odwrotny do logowania (ang. log out).
zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochron danych przed ich nieuprawnionym przetwarzaniem.
zbiór danych – każdy posiadający struktur zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

BURMISTRZ
Franciszek Lech Kwaśniewski

Oświadczenie
pracowników o zapoznaniu się z treścią
POLITYKI BEZPIECZEŃSTWA.

L.p	Nazwisko i imię	Data	Podpis
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			

Uwaga:
Złożenie podpisu stanowi jednocześnie zobowiązanie do stosowania zasad zawartych w tym dokumencie.