Wójt Gminy Burzenin
98-260 Burzenin, ul. Sieradzka 1
pow. sieradzki, woj. łódzkie

Zarządzenie Nr 125/2009
Wójta Gminy Burzenin
z dnia 01 lipca 2009 r.

w sprawie wprowadzenia polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t. j.: Dz. U. z 2001 r. Nr 142, poz. 1591; z 2002 r. Nr 23, poz. 220, Nr 62, poz. 558, Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 214, poz.1806; z 2003 r. Nr 80, poz. 717 i Nr 162, poz. 1568; z 2004 r. Nr 102, poz. 1055 i Nr 116, poz. 1203; z 2005 r. Nr 172, poz. 1441 i Nr 175, poz. 1457; z 2006 r. Nr 17, poz. 128 i Nr 181, poz. 1337; z 2007 r. Nr 48, poz. 327, Nr 138, poz. 974, Nr 173, poz. 1218; z 2008r. Nr 180, poz.1111, Nr 223, poz. 1458; z 2009r. Nr 52, poz. 420), art. 36 ust. 2, art. 39 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271;z 2004 r. Nr 25, poz.219 i Nr 33, poz. 285; z 2006 r. Nr 104, poz. 708 i poz. 711; z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia2004 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. z 2004 r. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1 Ustala się Politykę bezpieczeństwa informacji w brzmieniu załącznika Nr 1 oraz instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w brzmieniu załącznika Nr 2 do niniejszego zarządzenia.

§ 2 Wykonanie zarządzenia powierza się Sekretarzowi Gminy oraz Administratorowi Bezpieczeństwa Informacji.

§ 3. Traci moc Zarządzenie Nr 43/2008 Wójta Gminy Burzenin z dnia 10 marca 2008r. w sprawie wprowadzenia polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 4 Zarządzenie wchodzi w życie z dniem 1 lipca 2009 roku.

WÓJT
Barbara Daru

Załącznik nr 1
do Zarządzenia nr 125/2009
Wójta Gminy Burzenin
Z dnia 01.07.2009

POLITYKA BEZPIECZEŃSTWA INFORMACJI
Urzędu Gminy Burzenin
(dokument główny)

WSTĘP

Niniejsza Polityka Bezpieczeństwa Informacji wraz z dokumentami uzupełniającymi wprowadza zasady bezpieczeństwa informacji w Urzędzie Gminy Burzenin.

Zasady, procedury i wytyczne zawarte zarówno w Polityce Bezpieczeństwa Informacji jak i dokumentach uzupełniających obowiązują wszystkich pracowników, praktykantów, stażystów oraz wszystkie pozostałe osoby, które posiadają lub z określonych przyczyn uzyskają dostęp do informacji chronionych przetwarzanych w Urzędzie Gminy Burzenin. Wszystkie z wymienionych osób zobowiązane są do zapoznania i bezwzględnego przestrzegania zasad i wytycznych niniejszej polityki.

Szczególną uwagę należy zwrócić na to, że nieznajomość Polityki Bezpieczeństwa Informacji nie zwalnia z obowiązku jej przestrzegania, a tym samym z odpowiedzialności, jaka z niej wynika.

Niezastosowanie się do Polityki Bezpieczeństwa Informacji stosowanej w Urzędzie Gminy Burzenin bądź naruszenie jej postanowień może być traktowane jako ciężkie naruszenie obowiązków pracownika i skutkować rozwiązaniem umowy o pracę bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.

Wszystkie dokumenty związane z bezpieczeństwem informacji przeznaczone są tylko i wyłącznie do użytku wewnętrznego.

1. Definicje i pojęcia

Ilekroć w polityce bezpieczeństwa jest mowa o:

- „ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, zwaną dalej „ustawą"; "[uodo[1]];
- administratorze danych - rozumie się przez to organ, instytucję, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ust. 1 i 2, decydujące o celach i środkach przetwarzania danych osobowych;
- „poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom" [rmswia];
- „przetwarzaniu danych – rozumie się przez to 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" [uodo];
- „systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych" [uodo];
- „haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym" [rmswia[2]];
- administratorze systemu – rozumie się przez to osobę odpowiedzialną za prawidłowe funkcjonowanie systemu przetwarzania danych [TISM[3]];
- autoryzacji – rozumie się przez to proces sprawdzenia prawa podmiotu do danego zasobu;
- danych osobowych – rozumie się przez to „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej" [uodo];
- administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez administratora danych zobowiązaną do stosowania środków technicznych i organizacyjnych zapewniających ochronę danych

---

[1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

[2] [rmswia] – Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[3] Total Information Security Management

osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną [uodo];

- identyfikatorze użytkownika – rozumie się przez to nazwę użytkownika w systemie przetwarzania informacji [TISM];
- integralności danych (informacji) – rozumie się przez to właściwość zapewniającą, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom [PN-I-1335-1:1999[4]];
- rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi [PN-I-1335-1:1999];
- integralności systemu – rozumie się przez to cechę polegającą na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej przez system zamierzonej funkcji w sposób wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej [PN-I-1335-1:1999];
- polityce bezpieczeństwa informacji – rozumie się przez to dokument określający metody i zasady ochrony informacji w organizacji [TISM];
- dostępności informacji – rozumie się przez to cechę zapewniającą, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba [TISM];
- uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu [rmswia];
- zbiorze (grupie) informacji chronionych – rozumie się przez to zbiór informacji podlegających ochronie, obejmujących podobne zagadnienia lub dotyczących jednego tematu; grupa informacji może być określona przepisami prawa [TISM];
- audycie bezpieczeństwa – rozumie się przez to czynności formalne mające na celu sprawdzenie, czy dane dokumenty lub systemy przetwarzania informacji spełniają założenia Polityki Bezpieczeństwa Informacji [TISM].

[4] [PN-I-13335-1:1999] – Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych.

2. Cel

Celem wdrożenia polityki bezpieczeństwa informacji w Urzędzie Gminy Burzenin jest zapewnienie bezpieczeństwa operacji związanych z ich przetwarzaniem oraz zgodności wszystkich procesów tego obszaru z obowiązującymi przepisami prawa zawartymi w ustawie oraz rozporządzeniu.

Niniejszy dokument zawiera niezbędny zbiór procedur do zapewnienia bezpieczeństwa odpowiedniego do rodzaju przetwarzanych informacji.

3. Strategia

3.1. W Urzędzie Gminy Burzenin przyjmuje się strategię zakładającą n/w zasady:
Każdy z pracowników, w tym szczególnie nowozatrudnionych, który swoje obowiązki realizować będzie przy wykorzystaniu informacji chronionych, jest zobowiązany do znajomości:

- Ustawy o ochronie danych osobowych;
- Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Burzenin;
- Polityki Bezpieczeństwa Informacji Urzędu Gminy Burzenin.

3.2. Polityka bezpieczeństwa informacji będzie poddawana bieżącym aktualizacjom tak często jak będzie to konieczne.

3.3. Zmiany, o których mowa w punkcie ***3.2*** będą obowiązkowo wprowadzane zarządzeniem Wójta Gminy Burzenin.

3.4. Systemy informatyczne oraz ich zabezpieczenia poddawane będą bieżącym kontrolom oraz aktualizacjom.

3.5. Zabezpieczenia fizyczne będą, co najmniej raz na kwartał, poddawane stosownym przeglądom i kontrolom.

4. Grupy informacji chronionych

W ramach grup informacji chronionych ustala się jedną grupę informacji chronionych niniejszą polityką tj. „Grupę Danych Osobowych".

5. Zarządzanie bezpieczeństwem

Zarządzanie bezpieczeństwem informacji chronionych w Urzędzie Gminy Burzenin obejmuje informacje przetwarzane w systemach papierowych oraz informatycznych.

Zakres i sposoby zarządzania zróżnicowane są w zależności od systemu przetwarzania, uregulowane są niniejszą Polityką Bezpieczeństwa Informacji i obejmują wszelkie aspekty (organizacyjny i techniczny) związane z uwierzytelnianiem, prowadzące do zachowania poufności, integralności oraz dostępności informacji.

6. Ogólne zasady bezpieczeństwa

Na bezpieczeństwo w Urzędzie Gminy Burzenin składa się wiele czynników i aspektów w poszczególnych obszarach. Obszary te omówione zostały w dalszej części niniejszego dokumentu. Z uwagi na fakt podłączenia niemal wszystkich stanowisk przetwarzających dane osobowe do sieci lokalnej oraz dostęp przynajmniej jednego z tych stanowisk do sieci publicznej, ustala się dla nich wysoki poziom bezpieczeństwa przetwarzania danych osobowych zgodnie z § 6 ust. 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

6.1. Organizacja bezpieczeństwa

Za organizację bezpieczeństwa danych osobowych w Urzędzie Gminy Burzenin odpowiada Wójt Gminy Burzenin będący z mocy prawa Administratorem Danych Osobowych.

6.2. Administrator Bezpieczeństwa Informacji

Nadzór nad przestrzeganiem stosowania środków technicznych i organizacyjnych wspomagających ochronę informacji pełni Administrator

Bezpieczeństwa Informacji. Administratorem Bezpieczeństwa Informacji jest osoba do tego celu powołana przez Wójta Gminy Burzenin.

6.3. Bezpieczeństwo fizyczne

Na bezpieczeństwo fizyczne omawiane w niniejszym dokumencie składa się bezpieczeństwo fizyczne i środowiskowe:

- budynków, w których swoją działalność prowadzi Urząd Gminy Burzenin;
- pomieszczeń, w których swoją działalność prowadzi Urząd Gminy Burzenin;
- sprzętu wykorzystywanego w Urzędzie Gminy Burzenin;
- innych elementów infrastruktury technicznej Urzędu Gminy Burzenin.

W ramach niniejszej polityki bezpieczeństwa informacji ustala się obszary przetwarzania informacji chronionych. Za wyznaczenie tychże obszarów odpowiada Administrator Bezpieczeństwa Informacji. Pomieszczenia stanowiące obszary bezpieczne zawarte zostały w załączniku nr 8 do niniejszej Polityki Bezpieczeństwa Informacji.

Dostęp do pomieszczeń stanowiących obszary bezpieczne mogą mieć:

- upoważnieni pracownicy Urzędu Gminy Burzenin;
- osoby nie będące pracownikami na zasadach i w przypadkach określonych w części „Bezpieczeństwo osób trzecich";
- pozostali pracownicy Urzędu Gminy Burzenin w obecności osoby upoważnionej, w przypadku zaistnienia konieczności realizacji zadań służbowych jednakże czas przebywania powinien zostać ograniczony do minimum;
- osoby, których informacje są w tym pomieszczeniu przetwarzane obowiązkowo w obecności osoby upoważnionej.

W przypadkach nieokreślonych powyżej, przebywanie w obszarze bezpiecznym wymaga pisemnej zgody Administratora Bezpieczeństwa Informacji.

6.3.1 Zabezpieczenie budynków

Budynki, w których prowadzi swoją działalność Urząd Gminy

Burzenin poza godzinami urzędowania muszą być bezwzględnie zabezpieczone w sposób uniemożliwiający przedostanie się do nich osób nieupoważnionych, poprzez stworzenie tzw. bariery bezpieczeństwa. Na zabezpieczenie budynków składa się:

- zabezpieczenie wejść do budynków,
- zabezpieczenie włazów dachowych,
- zabezpieczenie okien.

6.3.2 Zabezpieczenie pomieszczeń

W ramach zabezpieczenia pomieszczeń ustala się zasady ich zabezpieczania:

a) w godzinach urzędowania,

b) poza godzinami urzędowania.

Na zabezpieczenia pomieszczeń składa się:

- zabezpieczenie wejść,
- zabezpieczenie okien.

Rozmieszczenie urządzeń przetwarzających informacje chronione powinno eliminować:

- podejrzenie informacji wyświetlanych na monitorze,
- podejrzenie informacji na wydrukach,
- możliwość kradzieży wydruków lub nośników informacji.

Na czas opuszczenia pomieszczenia nakłada się na pracowników obowiązek zamknięcia okien oraz drzwi, zabezpieczenia wszystkich dokumentów oraz nośników.

Po zakończeniu pracy dokumentacja, nośniki wraz z innymi elementami wykorzystywanymi do przetwarzania informacji chronionych powinny zostać zabezpieczone przed dostępem osoby nieuprawnionej.

6.3.3 Bezpieczeństwo komputerów

W celu dotrzymania celu niniejszej polityki urzędowe komputery powinny być odpowiednio zabezpieczone. Zakres, rodzaj i sposób zabezpieczeń podyktowany jest rodzajem przetwarzanych informacji. Na minimalne zabezpieczenia komputerów składają się:

- hasła do biosu;
- hasła do systemów operacyjnych;
- skanery antywirusowe.

Opcjonalnym zabezpieczeniem komputerów jest zainstalowanie oprogramowania pełniącego funkcję firewall'a.

6.4 Bezpieczeństwo osobowe

Każdemu z pracowników przyznawane/odbierane są prawa dostępu do systemów informatycznych przetwarzających informacje chronione z wykorzystaniem wniosku złożonego przez kierownika komórki organizacyjnej do Administratora Danych Osobowych. Pracownikom przyznawane będą minimalne prawa dostępu do systemu pozwalające zarazem wykonywać powierzone obowiązki.

Do celów rekrutacji pracownik kadr opracowuje regulamin rekrutacji zawierający zasady weryfikacji osób ubiegających się o pracę.
Szczegółowe wytyczne dotyczące bezpieczeństwa osobowego zawarte zostały w instrukcji „Bezpieczeństwo osobowe" stanowiącej załącznik nr 2 do niniejszej Polityki Bezpieczeństwa Informacji.

6.4.1 Bezpieczeństwo osób trzecich

Dostęp do informacji chronionych, systemów je przetwarzających, urządzeń wspomagających przetwarzanie, a w szczególności komputerów posiadają jedynie pracownicy zatrudnieni w Urzędzie Gminy Burzenin posiadający stosowne upoważnienia.

Osoby trzecie mogą mieć dostęp do w/w elementów tylko i wyłącznie w następujących przypadkach:

- gdy pełnią funkcje kontrolne (posiadając odpowiednie dokumenty w postaci wniosków, upoważnień i legitymacji oraz pisemnego powodu i zakresu kontroli, zawierające co najmniej:
  a) wskazanie przepisów uprawniających do dostępu do informacji;
  b) wskazanie rodzaju i zakresu informacji oraz formy ich udostępnienia;

c) wskazanie imienia, nazwiska i funkcji osoby, której dane mają być udostępnione).

- po spełnieniu powyższych formalności dane przekazuje się za potwierdzeniem odbioru,
- gdy są pracownikami firmy serwisującej sprzęt komputerowy pod warunkiem, że naprawa wykonywana jest przy udziale Administratora Bezpieczeństwa Informacji; jeśli naprawa okaże się niemożliwa do zrealizowania w siedzibie Urzędu Gminy Burzenin i zaistnieje konieczność wyniesienia sprzętu poza obszar, w którym jest on wykorzystywany - dysk twardy zostanie wymontowany i zabezpieczony.

  W przypadku konieczności przekazania komputera wraz z dyskiem zawierającym informacje chronione uregulowane zostanie to odrębną umową zawierającą oświadczenie o zachowaniu poufności informacji wraz ze wskazaniem sankcji za niedotrzymanie tajemnicy wynikającej z umowy.

  W przypadku wymiany danych z instytucjami bądź innymi podmiotami stosowane będą umowy zawierające klauzule o zachowaniu tajemnicy oraz informacje o sankcjach za niedotrzymanie tajemnicy wynikającej z umowy.

7. Przetwarzanie informacji chronionych

Przetwarzanie informacji chronionych w Urzędzie Gminy Burzenin może odbywać się tylko i wyłącznie w systemach spełniających wymogi „Ustawy o ochronie danych osobowych", a ich archiwizacja (przechowywanie kopii) musi spełniać wymogi „Ustawy o archiwach".

8. Wymagania bezpieczeństwa dla systemów przetwarzania informacji

Wymagania dla systemów przetwarzania informacji są zróżnicowane i zależą od rodzaju przetwarzanych informacji oraz od innych czynników. Niniejszy dokument traktuje ogólnie kwestię bezpieczeństwa systemów przetwarzania. Precyzyjne informacje na ten temat znajdują się w opisach poszczególnych systemów.

8.1 Wymagania informatycznych systemów przetwarzania

Systemy informatyczne wykorzystywane do przetwarzania danych realizować założenia Polityki Bezpieczeństwa Informacji Urzędu Gminy Burzenin oraz w szczególności wymogi Ustawy o ochronie danych osobowych i aktów wykonawczych do niej wydanych. Podstawowe wymagania obejmują:

- uwierzytelnianie użytkowników;
- zasady bezpieczeństwa nośników;
- procedury archiwizacji;
- zasady bezpieczeństwa systemów przetwarzania;
- politykę antywirusową;
- zabezpieczenie komputerów oraz określenie zasad ich wykorzystania;
- określenie zasad dostępu do sieci publicznej.

8.2 Wymagania papierowych systemów przetwarzania

Systemy tradycyjne (papierowe) wykorzystywane do przetwarzania danych realizować założenia Polityki Bezpieczeństwa Informacji Urzędu Gminy Burzenin. Podstawowe wymagania obejmują:

- zasady przechowywania dokumentów,
- zasady niszczenia dokumentów.

9. Postępowanie w sytuacjach naruszenia bezpieczeństwa

Naruszenie bezpieczeństwa informacji z uwagi na priorytet sprawy traktowane jest bardzo ważny elementem bezpieczeństwa informacji. Szczegóły dotyczące naruszenia bezpieczeństwa informacji określone zostały w instrukcji „Naruszenie bezpieczeństwa informacji" będącej załącznikiem nr 6 do niniejszej polityki.

10. Wykaz załączników

1. Ochrona antywirusowa.
2. Bezpieczeństwo osobowe.
3. Użytkowanie nośników informacji.
4. Niszczenie nośników informacji.
5. Kopie zapasowe.

6. Naruszenie bezpieczeństwa informacji.
7. Wytyczne kontroli i audytu.
8. Wykaz budynków i pomieszczeń stanowiących obszary chronione.
9. Wykaz zbiorów.

Wykaz dokumentów

Politykę Bezpieczeństwa Informacji Urzędu Gminy Burzenin opracowano w oparciu o następujące dokumenty:

- Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. z 1999 r. Nr 18, poz. 162);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);
- Rozporządzenie Prezesa rady Ministrów z dnia 22 grudnia 1999 roku w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych (Dz. U. z 1999 r. Nr 112, poz. 1319 z późn. zm.);
- Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. Nr 24, poz. 141 z późn. zm.);
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926);
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553 z dnia 2 sierpnia 1997 r.; sprostowanie: z 1997 r. Dz. U. Nr 128, poz. 840; zm.: z 1999 r. Nr 64, poz. 729 i Nr 83, poz. 931, z 2000 r. Nr 48, poz. 548 i Nr 93, poz. 1027);
- Ustawa z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.);
- PN-ISO/IEC 17799 : 2003, Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji;

- PN-I-13335-1 : 1999, Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych;
- ISO/IEC TR 13335-2 : 1997, Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Zarządzanie i planowanie bezpieczeństwa systemów informatycznych;
- ISO/IEC TR 13335-3 : 1998, Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – techniki zarządzania bezpieczeństwem systemów informatycznych;
- ISO/IEC TR 15947 : 2002 Technika informatyczna - Techniki zabezpieczeń – Struktura wykrywania włamań w systemach teleinformatycznych;
- Total Information Security Management ver. 1.4.

1. Cel

Określenie zasad ochrony antywirusowej w Urzędzie Gminy Burzenin.

2. Zakres stosowania i obszar działania

Wytyczne zawarte w procedurze obejmują swym oddziaływaniem wszystkie komputery oraz systemy informatyczne na nich wykorzystywane znajdujące się w Urzędzie Gminy Burzenin.

3. Treść

3.1 Instalacji oraz konfiguracji oprogramowania dokonuje tylko i wyłącznie informatyk.

3.2 Każdy komputer posiada zainstalowane oprogramowanie antywirusowe działające w trybie rzeczywistym.

3.3 Oprogramowanie musi posiadać opcje automatycznych aktualizacji baz i sygnatur wirusów.

3.4 Dla jednostek, które nie mają dostępu do serwerów aktualizacyjnych producenta oprogramowania tworzy się lokalną bazę sygnatur aktualizowaną nie rzadziej niż przewiduje to jej producent.

3.5 Oprogramowanie antywirusowe obejmuje swym działaniem wszystkie systemy wykorzystywane w Urzędzie Gminy Burzenin w tym szczególnie pocztę elektroniczną.

3.6 Zobowiązuje się użytkowników komputerów do zawiadomienia informatyka o komunikatach wysyłanych przez skaner.

1. Cel

Określenie zasad bezpieczeństwa w odniesieniu do osób z prawami dostępu do systemów przetwarzania informacji chronionych..

2. Zakres stosowania i obszar działania

Wytyczne zawarte w niniejszej instrukcji dotyczą wszystkich osób wymienionych w punkcie 1 niniejszej instrukcji.

3. Treść

3.1 Każda z osób wykonujących operacje w systemie(ach) przetwarzania informacji chronionych musi bezwzględnie posiadać upoważnienie uprawniające do pracy w systemie.

3.2 Wydanie upoważnienia poprzedza:

a) szkolenie obejmujące aspekty Ustawy o ochronie danych osobowych oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,,

b) szkolenie z zakresu Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych oraz Polityki Bezpieczeństwa Informacji,

c) złożenie oświadczenia o odbyciu szkolenia

d) złożenie oświadczenia o zachowaniu poufności informacji.

3.3 Upoważnienia obowiązują wszystkich pracowników, stażystów oraz praktykantów.

3.4 Wydanie oraz anulowanie upoważnienia następuje na wniosek sekretarza urzędu.

3.5 O przyznaniu praw dostępu decyduje Administrator Bezpieczeństwa Informacji na podstawie zakresu czynności, które wykonywała będzie dana osoba.

3.6 Upoważnienie wydaje oraz anuluje Wójt Gminy Burzenin.

3.6.1 Pracownik, któremu wydane zostało upoważnienie ponosi pełną odpowiedzialność za wykonywane operacje.

3.6.2 Upoważnienia wydawane pracownikom muszą być ewidencjonowane.

3.6.3 Ewidencję w formie rejestru prowadzi Administrator Bezpieczeństwa Informacji.

3.6.4 Rejestr upoważnień zawiera:

- ✓ imię i nazwisko pracownika,
- ✓ nazwę komórki organizacyjnej,
- ✓ zakres upoważnienia,
- ✓ datę wydania oraz anulowania upoważnienia,

3.7 Wgląd do rejestru upoważnień posiada jedynie Wójt Gminy Burzenin oraz Sekretarz Gminy Burzenin.

Wzór oświadczenia o zachowaniu poufności:

.....
(imię i nazwisko pracownika)

.....
(stanowisko)

Oświadczenie o zachowaniu poufności informacji

Ja niżej podpisana(y), świadoma(y) konsekwencji wynikających z zapisów Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz konsekwencji przewidzianych w Polityce Bezpieczeństwa Informacji Urzędu Gminy, zobowiązuję się dobrowolnie do zachowania poufności informacji pozyskanych w czasie wykonywania pracy oraz do niewykorzystywania ich do celów innych niż związane z wykonywaną pracą.

Do zachowania poufności informacji zobowiązuję się również po ustaniu mojego zatrudnienia w Urzędzie Gminy Burzenin.

.....
Data i podpis pracownika

Wzór oświadczenia o odbyciu szkolenia:

.....
(imię i nazwisko pracownika)

.....
(stanowisko)

Oświadczenie

Ja niżej podpisana(y) oświadczam, iż odbyłam(em) szkolenie w ramach, którego zapoznana(y) zostałam(em) z :

1. Ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
2. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 9 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
3. Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
4. Polityką Bezpieczeństwa Informacji.

Mając powyższe na uwadze zobowiązuję się do ścisłego przestrzegania w/w dokumentów.

.....
Data i podpis pracownika

Wzór rejestru upoważnień

Rejestr upoważnień

Lp.	Imię i nazwisko pracownika	Nazwa komórki organizacyjnej	Zakres upoważnienia	Opis zadań	Data wydania upoważnienia	Data anulowania upoważnienia

Wzór upoważnienia:

Upoważnienie Nr .....

Upoważniam Panią (Pana) ..... do przetwarzania danych osobowych w następujących zbiorach:

1) .....
(nazwa)

2) .....
(nazwa)

3) .....
(nazwa)

w zakresie:

Ad. 1.

.....

Ad. 2.

.....

Ad. 3.

.....

Przyznane prawa dostępu:

- ☐ - pełne uprawnienia
- ☐ - zapis
- ☐ - odczyt
- ☐ - edycja
- ☐ - drukowanie

Niniejsze upoważnienie obowiązuje od dnia ..... i ważnie jest do dnia.....

.....
(podpis)

1. Cel

Wprowadzenie zasad bezpiecznego użytkowania nośników informacji użytkowanych w Urzędzie Gminy Burzenin.

2. Zakres stosowania i obszar działania

Wytyczne zawarte w niniejszej instrukcji stosowane będą do wszystkich nośników informacji typu dysk twardy, dyskietka, pamięci przenośne, płyty CD i DVD, taśmy magnetyczne itp.

3. Treść

3.1 Na terenie Urzędu Gminy Burzenin obowiązuje zakaz użytkowania nośników informacji innych niż te które zostały zakupione przez Urząd Gminy Burzenin.

3.2 W oparciu o powyższy punkt ustala się, że wszystkie nośniki informacji znajdujące się na terenie Urzędu Gminy stanowią jego własność i mogą być wykorzystywane jedynie do celów służbowych.

3.3 Nośniki wykorzystywane w Urzędzie powinny być oznaczone według ustalonego schematu znakowania nośników.

3.4 Osoby wykorzystujące nośniki ponoszą za nie odpowiedzialność.

3.5 Za odpowiednie oznakowanie nośników odpowiada inspektor ds. ogólno-administracyjnych.

3.6 Na zewnętrznych nośnikach informatycznych zabrania się przechowywania całych baz danych zawierających dane osobowe.

3.7 Przypadek utraty bądź uszkodzenia nośnika zawierającego dane należy niezwłocznie w formie notatki służbowej poinformować Administratora Bezpieczeństwa Informacji.

3.8 W przypadku nośników informacji w postaci kartki papieru zabrania się ich powtórnego wykorzystania np. jako brudnopisy (np. druga strona niepoprawnie wydrukowanego dokumentu).

3.9 Nośniki, które użyte zostały do pracy z danymi osobowymi nie mogą być używane do innych celów.

3.10 Przed rozpoczęciem użytkowania nośnika informatycznego na terenie urzędu należy go dokładnie sprawdzić skanerem antywirusowym.

3.11 Po zakończeniu pracy nośniki informacji należy zabezpieczyć w przeznaczonych do tego miejscach.

3.12 Wszelkie druki nienadające się do użycia na koniec pracy należy zniszczyć w niszczarce.

	POLITYKA BEZPIECZEŃSTWA INFORMACJI – ZAŁĄCZNIK NR 4	Wersja 1.1
	NISZCZENIE NOŚNIKÓW INFORMACJI	Ilość stron: 1

1. Cel

Wprowadzenie zasad likwidacji nośników informacji.

2. Zakres stosowania i obszar działania

Wytyczne zawarte w niniejszej instrukcji stosowane będą do wszystkich nośników informacji..

3. Treść

3.1 Nośniki informacji stosowane w Urzędzie Gminy Burzenin w przypadku stwierdzenia ich zużycia podlegają zniszczeniu.

3.2 Decyzję o zlikwidowaniu nośnika podejmuje Administrator Bezpieczeństwa Informacji.

3.3 Nośnik przeznaczony do likwidacji powinien być przechowywany w przeznaczonym do tego miejscu.

3.4 Nośnik należy zniszczyć w sposób fizyczny, całkowicie uniemożliwiający odczytanie jakichkolwiek danych jakie na nim były przechowywane.

3.5 Po zlikwidowaniu nośnika należy sporządzić protokół zniszczenia zawierający:

a) datę likwidacji;
b) nazwę podmiotu dokonującego likwidacji;
c) opis nośnika i sposób jego likwidacji.

3.6 Protokół o którym mowa w punkcie **3.5** powinien być przechowywany przez Administratora Informacji.

1. Cel

Ustalenie zasad wykonywania kopii zapasowych.

2. Zakres stosowania i obszar działania

Wytyczne zawarte w niniejszej instrukcji dotyczą wszystkich systemów przetwarzania.

3. Treść – Archiwizacja danych

3.1. W Urzędzie Gminy Burzenin archiwizacji podlegają:

a) dane z komputerów wchodzących oraz nie wchodzących w obręb sieci lokalnej;

b) dane z serwera plików.

3.2. Osobą odpowiedzialną za archiwizację danych jest informatyk.

3.3. Za archiwizowanie danych z komputerów, wymienionych w pkt. **3.1** ust. **a** odpowiadają ich użytkownicy.

3.4. Nośniki zawierające kopie oznaczone są opisem według następującego schematu:

a) data i godzina wykonania kopii (dd.mm.rrrr - gg:mm);

b) podpis informatyka;

c) opis zawartości kopii lub symbol kopii zgodny z legendą zawartości.

3.5. Sposoby wykonywania kopii w Urzędzie Gminy Burzenin określi Administrator Bezpieczeństwa Informacji w odrębnej instrukcji.

3.6. Za utratę danych podlegających archiwizacji odpowiada osoba odpowiedzialna za ich wykonywanie.

4. Treść - Oprogramowanie

4.1. W zakresie oprogramowania stosowanego w urzędzie ustala się zasadę utworzenia kopii bezpieczeństwa o ile posiadana licencja tego nie zabrania.

4.2. Oryginalne nośniki z oprogramowaniem przechowywane są w wyznaczonym do tego miejscu.

1. Cel

Ustalenie sposobu postępowania w przypadku naruszenia bezpieczeństwa informacji bądź systemu przetwarzania.

2. Zakres stosowania i obszar działania

Wytyczne zawarte w niniejszej instrukcji dotyczą wszystkich informacji chronionych i systemów przetwarzania.

3. Treść

3.1 Naruszeniem bezpieczeństwa informacji w rozumieniu niniejszego dokumentu jest:

- przypadek nieautoryzowanego odczytu, modyfikacji, usunięcia oraz innych operacji na danych;
- przypadek naruszenia zabezpieczeń systemów;
- pozostawienie niezabezpieczonych dokumentów, nośników bądź sprzętu przetwarzającego dane;
- nieprawidłowe wykorzystanie bądź spowodowanie uszkodzeń sprzętu przetwarzającego dane osobowe bądź nośników informacji;
- pozostawienie w czasie pracy pomieszczenia, w którym przetwarzane są dane bez uprzedniego ich zabezpieczenia poprzez np. schowanie dokumentów papierowych lub zablokowanie dostępu do komputera przez chociażby wygaszacz ekranu zabezpieczony hasłem;
- pozostawienie niezabezpieczonego pomieszczenia w czasie pracy np. wyjście z pokoju i niezamknięcie okien lub drzwi;
- niestosowanie polityki czystego biurka tzn. rozmieszczenie dokumentów w sposób umożliwiający osobom nieuprawnionym łatwy dostęp do nich;
- niestosowanie polityki czystego ekranu tzn. ustawienie monitorów w taki sposób, aby uniemożliwić osobom nieuprawnionym podejrzenia informacji wyświetlanych na ekranie;

- pozostawienie nieuprawnionej osoby w pomieszczeniu stanowiącym obszar chroniony bez osoby posiadającej upoważnienie do przetwarzania danych w tym obszarze;
- próba nieautoryzowanego dostępu do informacji np. w celu wyrządzenia szkody bądź wykorzystania informacji w celu osiągnięcia korzyści majątkowych.

3.2 O naruszeniu bezpieczeństwa informacji bądź systemu przetwarzania należy niezwłocznie poinformować Administratora Bezpieczeństwa Informacji bądź Administratora Danych Osobowych.

3.3 Do tego czasu należy podjąć kroki mające na celu zapobieżenie dalszych negatywnych skutków tego działania.

3.4 Po podjęciu informacji o naruszeniu bądź podejrzeniu naruszenia bezpieczeństwa Administrator Danych bądź Administrator Bezpieczeństwa Informacji rozpoczynają czynności wyjaśniająco-sprawdzające.

3.5 W przypadku gdy okaże się to niezbędne Administrator systemu wstrzymuje niezwłocznie pracę systemu poprzez natychmiastowe odłączenie zasilania od komputera którego incydent dotyczy.

3.6 W przypadku braku możliwości dogłębnej analizy we własnym zakresie Administrator Bezpieczeństwa informacji podejmuje działania dotyczące przekazania sprawy specjalistycznej firmie.

3.7 O dalszych działaniach (np. powiadomieniu właściwych organów) decyduje Administrator Danych.

3.8 Osoba dopuszczająca się naruszenia bezpieczeństwa informacji ponosi odpowiedzialność na podstawie:

a) zapisów Polityki Bezpieczeństwa Informacji Urzędu Gminy Burzenin;
b) Kodeksu Karnego;
c) Ustawy o ochronie danych osobowych.

1. Cel

Ustalenie wytycznych do przeglądów okresowych zapobiegających naruszeniom obowiązku szczególnej staranności Administratora danych oraz wytycznych do audytu bezpieczeństwa informacji.

2. Zakres stosowania i obszar działania

Niniejsze wytyczne obejmują swym zakresem wszystkie aspekty bezpieczeństwa informacji.

3. Treść – przeglądy okresowe

3.1 Przynajmniej raz w roku Administrator Bezpieczeństwa Informacji dokonuje przeglądu przetwarzanych danych pod kątem celowości ich dalszego przetwarzania.

3.2 Zasadniczym celem przeprowadzania takiego przeglądu jest wskazanie danych, których cel przetwarzania został osiągnięty co wiąże się z usunięciem danych z uwagi na brak celu przetwarzania.

3.3 W przypadku stwierdzenia konieczności usunięcia danych sporządzany jest z tego protokół, na którym podpisy swe składają Administrator Bezpieczeństwa Informacji oraz kierownik jednostki.

4. Treść – audyt bezpieczeństwa informacji

4.1 Audyt bezpieczeństwa informacji powinien być przeprowadzany conajmniej raz w roku.

4.2 W ramach audytu dokonuje się kontroli:

a) praktycznego zastosowania Polityki Bezpieczeństwa Informacji;
b) kompletności Polityki Bezpieczeństwa Informacji;
c) zmian w budowie systemów informatycznych;
d) przeglądów zabezpieczeń.

4.3 Przeprowadzenie audytu bezpieczeństwa systemu możliwe jest jedynie po uzgodnieniu tego z administratorem systemu.

4.4 Audyt przeprowadza Administrator Bezpieczeństwa Informacji.

4.5 Przed rozpoczęciem audytu przedstawiany jest kierownikowi jednostki zakres audytu oraz jego harmonogram.

4.6 Wyniki audytu przedkładane są do zapoznania się kierownikowi jednostki i zawierają conajmniej:

- szczegółowy opis zadań audytorskich;
- szczegółowy opis zagrożeń;
- zalecenia pokontrolne wraz z ich uzasadnieniem oraz proponowanym terminem ich realizacji;
- opinie Administratora Systemu oraz Administratora Bezpieczeństwa Informacji.

WZÓR

W ramach Polityki Bezpieczeństwa Informacji ustala się poniższy wzór wykazu budynków i pomieszczeń stanowiących obszary bezpieczne.

WYKAZ BUDYNKÓW I POMIESZCZEŃ STANOWIĄCYCH OBSZARY BEZPIECZNE	
Adres budynku	Precyzyjna lokalizacja (pomieszczenia)

WZÓR

W ramach Polityki Bezpieczeństwa Informacji ustala się poniższy wzór wykazu zbiorów danych osobowych.

L.P.	Nazwa zbioru danych	Forma	Poziom bezpieczeństwa	Systemy informatyczne	Lokalizacja fizyczna	Pomieszczenia, w których przetwarzane są dane

Załącznik nr 2
do Zarządzenia nr 125/2009
Wójta Gminy Burzenin
Z dnia 01.07.2009

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

1. Cel instrukcji

Określenie sposobu zarządzania systemami informatycznym, służącymi do przetwarzania danych osobowych w Urzędzie Gminy Burzenin w celu zabezpieczenia danych osobowych.

2. Definicje

Ilekroć w instrukcji jest mowa o:

- administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji;
- administratorze danych – rozumie się przez to podmiot lub osobę określone w art. 3, Ustawy o ochronie danych osobowych;
- administratorze systemu – rozumie się przez to osobę odpowiedzialną za prawidłowe funkcjonowanie systemu przetwarzania danych;
- haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- identyfikatorze – rozumie się przez to ciąg znaków, które tworzą nazwę użytkownika w systemie informatycznym;
- integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych;
- poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

- przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy;
- rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- rozporządzeniu – rozumie się przez to Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- sieci publicznej – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne;
- sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (DzU nr 73, poz. 852 ze zm.);
- systemie informatycznym – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
- teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
- ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
- uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

– użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

3. Poziom bezpieczeństwa

Uwzględniając fakt podłączenia stanowisk wykorzystywanych do przetwarzania danych osobowych do sieci publicznej ustala się wysoki poziom bezpieczeństwa danych na podstawie § 6 ust. 4 Rozporządzenia ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

4. Uprawnienia w systemie informatycznym

4.1 Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie Gminy Burzenin może uzyskać osoba, która posiada upoważnienie do pracy na zbiorach danych osobowych.

4.2 Do pracy z systemem informatycznym niezbędne jest posiadanie dostępu do niego.

4.3 Dostęp do systemu realizowany jest na podstawie identyfikatora użytkownika oraz hasła do konkretnego systemu informatycznego.

4.4 Konto w systemie informatycznym zakłada Administrator Systemu na wniosek bezpośredniego przełożonego pracownika.

4.5 Wzór wniosku stanowi załącznik nr 1 do niniejszej instrukcji.

4.6 Poprzez założenie konta w systemie informatycznym rozumie się

a) ustalenie identyfikatora;

b) wprowadzenie hasła wraz z ustaleniem terminu jego ważności;

c) nadanie uprawnień.

4.7 W przypadku nieobecności dłuższej niż 10 dni roboczych bezpośredni przełożony pracownika informuje o tym Administratora Systemu poprzez złożenie wniosku o czasową blokadę konta.

4.8 W przypadku konieczności likwidacji konta bezpośredni przełożony informuje o tym niezwłocznie Administratora Systemu.

5. Uwierzytelnianie

5.1 Nazwa użytkownika (identyfikator) jest ciągiem znaków, z których pierwszy odpowiada pierwszej literze imienia, a pozostałe znaki odpowiadają literom nazwiska użytkownika. Z uwagi na zróżnicowanie systemów przyjmuje się zasadę niestosowania polskich znaków diakrytycznych oraz wielkich liter w nazwach użytkowników (identyfikatorach).

PRZYKŁAD: *Dla użytkownika Jana Kowalskiego identyfikator wygląda następująco jkowalski.*

5.2 Hasło składa się z minimum ośmiu unikalnych znaków znanych jedynie jego właścicielowi.

5.3 Hasło powinno składać się z kombinacji dużych i małych liter, cyfr oraz znaków specjalnych.

5.4 Konstrukcja hasła powinna być na tyle skomplikowana aby nie była łatwo kojarzona z użytkownikiem.

5.5 System informatyczny powinien wymuszać zmianę hasła co 30 dni oraz zapobiegać jego powtarzaniu się.

5.6 Pierwsze hasło użytkownik otrzymuje od Administratora Systemu i zobowiązany jest do jak najszybszej jego zmiany.

5.7 Zabrania się przekazywania haseł innym osobom oraz zapisywania ich na kartkach itp.

6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu

6.1 Użytkownik rozpoczyna pracę w systemie przetwarzania od uruchomienia komputera, podania hasła z poziomu BIOS oraz uwierzytelnieniu się w systemie operacyjnym.

6.2 Uwierzytelnienie w BIOS'sie polega na wprowadzeniu hasła użytkownika.

6.3 Przed uwierzytelnieniem w BIOS'sie oraz/lub systemie użytkownik powinien upewnić się czy inna osoba nie ma możliwości obserwowania wprowadzania haseł.

6.4 Uwierzytelnienie polega na podaniu indywidualnego identyfikatora użytkownika (nazwy użytkowania) oraz hasła.

6.5 W przypadku opuszczenia stanowiska pracy na krótki czas należy zawiesić pracę w systemie i zablokować konsolę systemu przez naciśnięcie CTRL+ALT+DEL i wciśnięcie przycisku „Zablokuj Komputer".

6.6 Po powrocie do swojego stanowiska pracy należy odblokować konsolę podając hasło.

6.7 Zakończenie pracy w systemie odbywa się przez wylogowanie z systemu oraz wyłączenie komputera.

6.8 Przed wylogowaniem z systemu należy upewnić się, że wszystkie wyniki pracy zostały zachowane.

6.9 Przed odejściem od stanowiska pracy należy upewnić się, że proces wylogowania zakończył się pomyślnie.

7. Procedury tworzenia kopii zapasowych

7.1 Wytyczne dotyczące wykonywania kopii zapasowych zawarte zostały w Polityce Bezpieczeństwa Informacji Urzędu Gminy Burzenin.

7.2 W ramach niniejszej instrukcji ustala się następujące metody wykonywania kopii zapasowych:

a) codziennie pełna kopia baz danych przechowywanych na serwerze;

b) w każdy czwartek o godzinie 22:00 kopia danych i aplikacji – takie podejście pozwala zweryfikować poprawność wykonania kopii oraz ewentualną korektę procesu archiwizacji przed rozpoczęciem pierwszego dnia roboczego kolejnego tygodnia;

c) ostatniego dnia roboczego miesiąca - pełna kopia wszystkich danych, aplikacji oraz systemu.

8. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

Wytyczne dotyczące zabezpieczeń przed działalnością szkodliwego oprogramowania zawarte zostały w Polityce Bezpieczeństwa Informacji.

9. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

9.1 Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.

9.2 Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) administrator systemu dokonuje nie rzadziej niż raz na tydzień.

9.3 Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale administratora systemu nie rzadziej niż raz na miesiąc.

9.4 Zapisy logów systemowych powinny być przeglądane przez administratora systemu codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

9.5 Kontrole i testy przeprowadzane przez administratora bezpieczeństwa informacji powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

10. Postanowienia końcowe

10.1 Niniejszy dokument ściśle uzupełnia się z Polityką bezpieczeństwa informacji Urzędu Gminy Burzenin.

10.2 Wytyczne dotyczące jego znajomości i obowiązku przestrzegania oraz konsekwencje zaniechania postanowień w nim zawartych są identyczne jak zawarte w w/w polityce.

Załącznik nr 1 do instrukcji

Wniosek o konto w systemie informatycznym

Zgodnie z instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych wnioskuję o: założenie/blokadę/usunięcie[1]

konta w systemie informatycznym

.....
(nazwa sytemu informatycznego)

dla

.....
(dane użytkownika)

pracującego z następującymi zbiorami danych osobowych

.....
(nazwa zbioru)

od dnia ..... do dnia .....

.....
(podpis bezpośredniego przełożonego)

[1] Niepotrzebne skreślić