ZARZĄDZENIE Nr B-0151/210/09
BURMISTRZA MIASTA BIERUNIA
z dnia 17.11.2009 r.

w sprawie: wprowadzenia w życie Księgi Bezpieczeństwa Systemu w Urzędzie Miejskim w Bieruniu.

Na podstawie art. 33 ust. 2 ustawy z dnia 8.03.1990 r. o samorządzie gminnym (tekst jednolity Dz. U. Nr 142, poz. 1591 z 2001 r. wraz z późniejszymi zmianami), w związku z art. 36 i następne ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101, poz. 926 z 2002 r. z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)

Postanawiam:

1. Wprowadzić w życie Księgę Bezpieczeństwa Systemu w Urzędzie Miejskim w Bieruniu w skład, której wchodzą:
   - Polityka Bezpieczeństwa Informacji,
   - Polityka Bezpieczeństwa Danych Osobowych,
   - Instrukcja Zarządzania Systemem Informatycznym

   wraz z załącznikami będącymi integralną częścią Księgi.

2. Uchylić Zarządzenie Nr B/112/2004 Burmistrza Miasta Bierunia z dnia 30.10.2004 r. w sprawie: polityki bezpieczeństwa informacji i instrukcji danych osobowych.

3. Wykonanie Zarządzenia powierzyć Sekretarzowi Miasta.

4. Zarządzenie wchodzi w życie z dniem podjęcia, z mocą obowiązującą od 1.12.2009 r.

Polityka Bezpieczeństwa Informacji

Spis treści

I Cel i zakres Polityki Bezpieczeństwa Informacji

1) Polityka Bezpieczeństwa Informacji dla Urzędu Miejskiego w Bieruniu w uporządkowanej formie opisuje działania organizacyjne i techniczne, których celem jest zapewnienie bezpieczeństwa organizacji, w tym przede wszystkim przetwarzanych informacji.
2) Polityka Bezpieczeństwa Informacji ustala zakresy obowiązków pracowników urzędu w procesie obiegu i ochrony informacji.
3) Polityka Bezpieczeństwa Informacji wraz z dokumentami Polityki Bezpieczeństwa Danych Osobowych, Instrukcją Zarządzania Systemem Informatycznym oraz dokumentami i wykazami w nich określonych tworzy Księgę Bezpieczeństwa Systemu w Urzędzie Miejskim w Bieruniu.
4) Niniejsza Polityka ma status dokumentu przeznaczonego do użytku wewnętrznego pracowników urzędu i może być udostępniona osobom postronnym jedynie za zgodą Burmistrza.

II Informacje wstępne

II.1 Podstawa prawna i źródła

Polityka Bezpieczeństwa Informacji uwzględnia wymagania dotyczące zarządzania bezpieczeństwem informacji zawarte w odpowiednich aktach prawnych oraz normach krajowych i międzynarodowych. W szczególności realizuje wymagania zawarte w:

1) Ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. 2002 r. Nr 101, poz. 926, ze zm.),
2) Ustawie o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994r. (Dz. U. 1994r. Nr 24, poz. 83),
3) Ustawie o dostępie do informacji publicznej z dnia 6 września 2001r. (Dz. U. 01.112.1198),
4) Ustawie o ochronie baz danych z dnia 27 lipca 2001r. (Dz. U. z 2001 r. Nr 128, poz. 1402),
5) Rozporządzeniu Prezydenta Rzeczypospolitej Polskiej z dnia 29 maja 1998r. (Dz. U. Nr 73, poz. 464) w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych,
6) Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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),
7) Normie PN-ISO/IEC 17799:2007: Technika informatyczna, Techniki Bezpieczeństwa, Praktyczne zasady zarządzania bezpieczeństwem informacji,
8) Normie PN-I-13335-1:1999: Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.

II.2 Definicje

Administrator Danych Osobowych [ADO]	rozumie się przez to Burmistrza Miasta Bierunia,
Administrator Bezpieczeństwa Informacji [ABI/ZABI]	powołana pisemnie przez ADO osoba, która w imieniu ADO sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych,
Administrator Systemu Informatycznego [ASI]	osoba odpowiedzialna za budowę, rozwój, modyfikację, wdrażanie oraz utrzymanie systemu informatycznego,
Osoba upoważniona	każda osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez ADO,
Użytkownik systemu	każda osoba, posiadająca upoważnienie do przetwarzania danych wydane przez ADO zarejestrowana w systemie /posiadająca unikalny identyfikator i hasło/ przetwarzająca dane osobowe
Dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych

	czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
Zbiór danych	rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
Przetwarzanie 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,
Usuwanie danych	rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
Identyfikator użytkownika	rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
Hasło	rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
Uwierzytelnianie	rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
Bezpieczeństwo informacji	zachowanie poufności, integralności i rozliczalności informacji
Poufność	właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom [ISO/IEC 13335-1:2004]
Poufność danych	rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
Dostępność	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu [ISO/IEC 13335-1:2004]
Integralność danych	rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
Rozliczalność	rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
Naruszenie danych osobowych	rozumie się przez to nielegalne ujawnienie, pozyskanie, nieuzasadnioną modyfikację lub zniszczenie danych osobowych, niepowołany dostęp
Naruszenie Polityki Bezpieczeństwa	rozumie się przez to działanie niezgodne z przyjętymi dokumentami polityki bezpieczeństwa
Polityka Bezpieczeństwa Informacji	wyrażona przez kierownictwo ogólna intencja i kierunki działań dotycząca bezpieczeństwa informacji Polityka Bezpieczeństwa Informacji
Sieć publiczna	rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
Sieć telekomunikacyjna	rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
Strona trzecia	to osoba lub organ, która w przypadku rozstrzygania

	problemu, jest uważana za niezależną od zaangażowanych stron [ISO/IEC Guide 2:1996]
System bezpieczeństwa	zestaw aktywów odpowiedzialnych za zabezpieczenie danych przed nieautoryzowanym dostępem wraz z organizacją i przyjętą dokumentacją w zakresie bezpieczeństwa.
System informatyczny	rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
Zabezpieczanie danych w systemie informatycznym	rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
Zagrożenie	potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji [ISO/IEC 13335-1:2004]

II.3 Odpowiedzialność

II.3.a Administrator Danych Osobowych

Administratorem Danych jest Burmistrz Miasta Bierunia.

Administrator jest odpowiedzialny za:

1) zabezpieczenie systemu przetwarzania danych osobowych w tym systemu informatycznego,
2) prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych,
3) dopuszczenie osób do pracy w systemie,
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych oraz do przebywania w pomieszczeniach w których przetwarzane są dane osobowe wraz z zakresami upoważnień,
5) formalną inicjację kontroli systemu informatycznego.

II.3.b Administrator Bezpieczeństwa Informacji /ABI/ oraz Zastępca Administratora Bezpieczeństwa Informacji /ZABI/

Na podstawie Art. 36 ust. 3 Ustawy o ochronie danych osobowych, Administrator Danych Osobowych powołał, zarządzeniem nr ____ z dnia _____, Administratora Bezpieczeństwa Informacji oraz Zastępcę Administratora Bezpieczeństwa Informacji.

Administrator Bezpieczeństwa Informacji oraz Zastępca Administratora Bezpieczeństwa Informacji są pracownikami etatowymi Urzędu Miejskiego. ABI oraz ZABI mają obowiązek zagwarantować w godzinach pracy systemu możliwość kontaktu ze sobą lub osobą posiadającą pisemne upoważnienie Administratora Bezpieczeństwa Informacji do podejmowania czynności w związku z uszkodzeniem, awarią bądź naruszeniem bezpieczeństwa.

Do zakresu odpowiedzialności ABI należy:

1) zapewnienie, aby do danych osobowych miały dostęp wyłącznie osoby upoważnione w zakresie wykonywanych zadań,
2) nadzorowanie fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe oraz kontroli przebywających w nich osób,

3) nadzorowanie przestrzegania zasad określonych w Polityce i Instrukcji dotyczących ochrony bezpieczeństwa danych osobowych,
4) nadzorowanie zasad i procedur wymienionych w Księdze Bezpieczeństwa Systemu oraz ich przestrzegania,
5) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
6) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych, jeśli takie wystąpiło, i przygotowanie oraz przedstawienie ADO odpowiednich zmian do Polityk Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym,

Do zakresu zadań Zastępcy Administratora Bezpieczeństwa Informacji należą w szczególności:

1) nadzorowanie zasad i procedur wymiany danych w sieci,
2) nadzorowanie obiegu dokumentów zawierających dane osobowe,
3) nadzorowanie funkcjonowania zasad i procedur związanych z uwierzytelnianiem użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych,
4) zlecenie modyfikacji uprawnień w systemach informatycznych w przypadku odebrania lub zmiany upoważnienia do przetwarzania danych osobowych,
5) szkolenie osób dopuszczonych do przetwarzania danych osobowych z zakresu przepisów prawa oraz uregulowań wewnętrznych w zakresie bezpieczeństwa danych osobowych,
6) nadzorowanie podpisania umów o poufności z użytkownikami upoważnionymi do przetwarzania danych osobowych, firmami, w tym firmami, którym powierzono przetwarzanie danych osobowych lub konserwacje urządzeń służących do przetwarzania danych oraz pracownikami tych firm.
7) Przejęcie obowiązków ABI w pełnym zakresie podczas jego nieobecności.

II.3.c Administrator Systemu Informatycznego

Zarządzeniem nr ____ z dnia _____, został powołany Administrator Systemu Informatycznego ze wskazaniem urządzeń oraz elementów systemu, do których jest dopuszczony w tym charakterze.

Do obowiązków Administratora Systemu Informatycznego należy:

1) wykonywanie czynności wynikających z Instrukcji w zakresie zabezpieczenia prawidłowego i bezpiecznego funkcjonowania bazy technicznej i oprogramowania systemu,
2) wprowadzenie lub usuwanie prawa dostępu do systemu informatycznego dla poszczególnych pracowników – z polecenia ADO,
3) opracowanie systemu haseł do poszczególnych obszarów systemu, zgodnie z wytycznymi zawartymi w Instrukcji Zarządzania Systemem Informatycznym,
4) zapewnienie konfiguracji systemu uniemożliwiającej wprowadzanie lub uzyskiwanie danych z systemu przez niepowołane osoby,
5) przeprowadzanie kontroli systemu informatycznego na wniosek ZABI,

6) monitorowanie bezpieczeństwa dla serwerów oraz urządzeń aktywnych sieci,
7) opracowywanie tematyki szkoleń z zakresu systemu oraz urządzeń dla użytkowników systemu – ze szczególną dbałością o wiedzę z zakresu bezpieczeństwa systemów.

II.3.d Osoba upoważniona – użytkownik systemu

W przetwarzaniu danych osobowych w Urzędzie, niezależnie od formy przetwarzania, biorą udział wyłącznie osoby posiadające pisemne upoważnienie nadane przez Administratora Danych Osobowych.

Użytkownikiem systemu informatycznego jest osoba, która w ramach swoich obowiązków służbowych korzysta z systemu informatycznego.

III Polityka Bezpieczeństwa Informacji

III.1 Deklaracja Burmistrza Miasta Bierunia

Mając świadomość znaczenia informacji i systemów informacyjnych dla realizacji zadań i celów Urzędu Miejskiego w Bieruniu deklaruję, że podejmowane przez pracowników Urzędu działania, dążą do zapewnienia bezpieczeństwa informacji zgodnymi z przepisami prawa, w tym w szczególności ustawą o ochronie danych osobowych oraz powszechnie stosowanymi normami bezpieczeństwa informacji, w szczególności z normą PN-ISO/IEC 17799:2007 „Praktyczne zasady zarządzania bezpieczeństwem informacji".

III.2 Podstawowe zasady bezpieczeństwa Informacji

1) W celu zapewnienia bezpieczeństwa przetwarzanych informacji stosuje się następujące ogólne zasady:

   a) „minimalnych przywilejów" – tzn. przydzielania praw dostępu tylko w zakresie niezbędnym do wykonania określonego zadania,
   b) „separacji obowiązków" - polegającej na tym, że zadania krytyczne z punktu widzenia bezpieczeństwa informacji nie mogą być realizowane przez jedną osobę,
   c) „domniemanej odmowy" - tzn. przyjęcia, jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach - „to, co nie jest dozwolone, jest zabronione".

2) Każdy pracownik Urzędu uczestniczący w przetwarzaniu danych osobowych posiada pisemne imienne upoważnienie wydane przez ADO.
3) System informatyczny jest zabezpieczony przed nieupoważnionym dostępem, modyfikacją lub zniszczeniem. Sieć wewnętrzna jest zabezpieczona przed nieupoważnionym dostępem z zewnątrz.
4) Informacje Urzędu są chronione w sposób proporcjonalny do ich wrażliwości, zagrożeń lub wymagań stawianych przez odpowiednie przepisy prawne.
5) Każdy pracownik dysponuje indywidualnym identyfikatorem za pośrednictwem, którego może korzystać z udostępnianych zasobów i usług. Włączone w systemie informatycznym mechanizmy oraz procedury zapewniają rozliczalność użytkowników zarejestrowanych w systemie.
6) Wszyscy pracownicy są zaznajomieni z przyjętą Polityką. Okresowo przeprowadzane są szkolenia dotyczące bezpieczeństwa informacji i ochrony danych osobowych.
7) Każdy pracownik Urzędu ma obowiązek informowania ABI za pośrednictwem bezpośredniego przełożonego o wystąpieniu incydentu związanego z bezpieczeństwem informacji.
8) W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji, kierownictwo Urzędu podejmie stosowne działania zaradcze w celu zmniejszenia potencjalnych strat.

IV Zarządzanie Bezpieczeństwem Informacji

Informacje, procesy wspierające, systemy informatyczne oraz sieci stanowią dla Urzędu istotną wartość. Poufność, integralność oraz dostępność informacji może odgrywać kluczową rolę w utrzymywaniu zgodności z obowiązującym prawem oraz wizerunku Urzędu.

Zależność od systemów informatycznych oraz od usług oznacza, że Urząd jest bardziej podatny na zagrożenia bezpieczeństwa. Połączenie sieci prywatnych oraz publicznych, a także dzielenie się zasobami informacyjnymi utrudniają osiągnięcie kontroli dostępu. Bezpieczeństwo osiągalne przez zastosowanie środków technicznych jest ograniczone i powinno być wspierane poprzez odpowiednie zarządzanie i procedury.

Zarządzanie bezpieczeństwem informacji wymaga, jako niezbędnego minimum, uczestnictwa wszystkich pracowników Urzędu Miejskiego.

IV.2 Struktura zarządzania bezpieczeństwem informacji

Zarządzanie Bezpieczeństwem Informacji wymaga ciągłego nadzorowania i monitorowania istniejących zagrożeń oraz stanu stosowanych zabezpieczeń. Za wprowadzenie zasad bezpieczeństwa informacji odpowiedzialność ponoszą wszyscy: Naczelnicy Wydziałów, Kierownicy Referatów i samodzielni pracownicy.

Dla celów sprawnego prowadzenia procesu zarządzania bezpieczeństwem, powołuje się Forum Zarządzania Bezpieczeństwem Informacji.

IV.2.a Skład Forum Zarządzania Bezpieczeństwem Informacji

W skład forum wchodzą:

1) Burmistrz Miasta – Administrator Danych Osobowych
2) Skarbnik Miasta
3) Sekretarz Miasta
4) Administrator Bezpieczeństwa Informacji
5) Zastępca ABI
6) Pełnomocnik ds. ochrony informacji niejawnych
7) Pracownicy powołani przez ADO

IV.2.b Zadania Forum Zarządzania Bezpieczeństwem Informacji

Podstawowym zadaniem Forum Zarządzania Bezpieczeństwem Informacji jest promowanie bezpieczeństwa wewnątrz Urzędu za pomocą odpowiedniego zaangażowania oraz dostępnych środków organizacyjnych i technicznych.

Forum Zarządzania Bezpieczeństwem Informacji zbiera się przynajmniej raz na pół roku w celu omówienia dotychczasowych zabezpieczeń oraz dokonuje analizy zdarzeń niebezpiecznych z poprzedniego okresu, a także podejmuje zadania:

1) prowadzi przegląd Polityki Bezpieczeństwa Informacji oraz ogólnej odpowiedzialności,
2) monitoruje zmiany w istotnych zagrożeniach zasobów informacyjnych,
3) prowadzi przeglądy i monitoring incydentów związanych z bezpieczeństwem informacji w systemach informatycznych oraz zbiorach tradycyjnych,
4) uzgadnia konkretne metodologie i procesy dotyczące poprawy bezpieczeństwa informacji, np.: ocena ryzyka, system klasyfikacji bezpieczeństwa,
5) uzgadnia i wspiera inicjatywy dotyczące poprawy bezpieczeństwa w Urzędzie, np.: program szkoleń w tym zakresie,
6) ocenia adekwatność oraz koordynuje wprowadzanie konkretnych środków kontroli bezpieczeństwa dotyczących nowych systemów czy usług,
7) tworzy listę zdarzeń niebezpiecznych dla każdego obszaru bezpieczeństwa,
8) proponuje zmiany do dokumentu Polityki Bezpieczeństwa Informacji i po zatwierdzeniu przez ADO zapoznaje z nimi wszystkich pracowników.

IV.3 Narzędzia i Metody Zarządzania

IV.3.a Norma PN-ISO/IEC 17799:2007

Niniejsza norma podaje zalecenia dla zarządzania bezpieczeństwem informacji do wykorzystania przez wszystkich, którzy są odpowiedzialni za inicjowanie, wdrażanie lub utrzymywanie bezpieczeństwa w Urzędzie. Zamiarem jest dostarczenie wspólnej bazy dla opracowywania wytycznych bezpieczeństwa i efektywnej praktyki zarządzania bezpieczeństwem informacji oraz zapewnienie zaufania w stosunkach między różnymi organizacjami.

Wybór zaleceń niniejszej normy odpowiada potrzebom Urzędu i jest zgodny z obowiązującym prawem i przepisami.

IV.3.b Ocena zagrożeń bezpieczeństwa informacji

Wymogi bezpieczeństwa określa się poprzez metodyczną ocenę zagrożeń bezpieczeństwa. Wydatki na środki kontroli muszą odpowiadać szkodom, jakie mogą wyniknąć w przypadku niezadziałania systemu bezpieczeństwa. Techniki oceny ryzyka można zastosować w całym Urzędzie, lub tylko w jej częściach; jak również w poszczególnych systemach informatycznych, konkretnych komponentach systemu lub w usługach, gdzie jest to praktyczne, realistyczne oraz pomocne.

Ocena ryzyka to systematyczne rozważanie:

1) szkód, w odniesieniu do przedmiotu działalności, których prawdopodobieństwo wystąpienia zachodzi na skutek niezadziałania systemu bezpieczeństwa, biorąc pod uwagę utratę poufności, pewności lub dostępności informacji i innych zasobów,
2) realnego prawdopodobieństwa takiego niezadziałania w świetle istniejących zagrożeń oraz podatności na nie, a także zastosowanych aktualnie środków kontroli.

IV.3.c Wybór środków kontroli

Po identyfikacji wymogów bezpieczeństwa dla Urzędu dokonano wyboru środków bezpieczeństwa i wprowadza się je w życie w celu zapewnienia, że ryzyka zostały sprowadzone do akceptowalnego poziomu.

IV.3.d Zarządzanie incydentami

Zarządzanie incydentami zapewnia szybkie, efektywne i uporządkowane reagowanie na incydenty związane z bezpieczeństwem informacji.

Wszelkie odkryte nieprawidłowości, związane z bezpieczeństwem Urzędu, jak i bezpieczeństwem informatycznym zgłaszane są, Zastępcy Administratora Bezpieczeństwa Informacji oraz Administratorowi Systemu Informatycznego.

Nadzór nad systemem uprawnień gwarantuje, że:

a) wyłącznie wyznaczony i uprawniony personel posiada dostęp do systemów i danych.
b) wszystkie działania awaryjne są w pełni udokumentowane.
c) działania awaryjne są zgłaszane są przełożynym i poddawane przeglądom przez Forum.

IV.4 Plan ciągłości działania

Plan ciągłość działania powinien rozpoczynać się od określenia wydarzeń mogących spowodować przerwy w przetwarzaniu informacji np. pożar czy powódź. Następnie należy przeprowadzić ocenę ryzyka w celu ustalenia skutków takich przerw (zarówno pod względem ewentualnych szkód jak i czasu powrotu do normalnego działania). Obie te czynności powinno się przeprowadzić z pełnym udziałem użytkowników zasobów. Ocena ta nie powinna ograniczać się tylko do urządzeń przetwarzania informacji.

Należy dążyć do zmniejszenia przerw w normalnym działaniu, spowodowanych przez nieszczęścia lub awarie zabezpieczeń (mogących być skutkiem klęsk żywiołowych, wypadków, awarii sprzętowych i umyślnych działań), do akceptowalnego poziomu poprzez zastosowanie środków zapobiegawczych i naprawczych. Dlatego też należy analizować potencjalne konsekwencje awarii systemu zabezpieczenia i utraty danych oraz opracować i wprowadzić takie plany awaryjne, by te dane zostały przywrócone w określonym czasie. Plany trzeba utrzymywać i ćwiczyć ich realizację, aby stały się one integralną częścią procesów zarządzania.

Na wypadek wystąpienia sytuacji kryzysowej postępować zgodnie z Planem reagowania Kryzysowego Urzędu Miejskiego w Bieruniu

V Postanowienia końcowe

Wszelkie zmiany wprowadzane są do polityki w formie aneksów opracowanych przez Forum Zarządzania Bezpieczeństwem Informacji i wdrażane odpowiednim zarządzeniem Burmistrza.

Polityka Bezpieczeństwa Informacji wraz z dokumentami powiązanymi wchodzi w życie z dniem 1 grudnia 2009.

Polityka Bezpieczeństwa Danych Osobowych

Spis treści

I Cel i zakres Polityki Bezpieczeństwa Danych Osobowych

Celem tej polityki jest wskazanie działań, jakie należy wykonać według ustalonych zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926, ze zm.).

Przez bezpieczeństwo danych osobowych rozumie się takie zabezpieczenie danych osobowych, poprzez wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych osobowych przetwarzane w Urzędzie, zarówno w formie elektronicznej za pomocą systemów informatycznych, jak i w formie papierowej. W zakresie podmiotowym Polityka obowiązuje wszystkich użytkowników przetwarzających dane osobowe.

II Wykaz budynków i pomieszczeń przetwarzania danych osobowych

Jako miejsce przetwarzania danych osobowych wyznacza się budynki Urzędu Miejskiego w Bieruniu, zlokalizowane przy Rynek 14 (segment A) i 15 (segment B) oraz pomieszczenia Straży Miejskiej w Bieruniu zlokalizowane w budynku przy ul. Władysława Jagiełły 1.

Segment A

Nr pomieszczenia:	1,2,3,4,5,.6	- WSO, USC
	7	- Radca Prawny
	8	- Sala narad
	9,10,11	- Sekretariat, Gabinet Burmistrza, Wiceburmistrza
	12	- Sekretarz Miasta
	13,14,16	- BOSiR
	15	- ZP
	17,18,20	- GPN
	23,24,25	- IMiR

Segment B

Nr pomieszczenia:	3,4,5,7	- ADM
	6	- BOSiR
	8,9,10,11	- FN
	12	- Skarbnik
	13	- Biuro Rady
	14	- Przew. Z-ca Przew. Rady Miasta
	15	- Duża sala szkoleń
	18,19,20,22	- GK
	23	- Mała sala szkoleń
	24	- Referat Informatyki
	25	- OSRiL
	28	- Promocja Miasta
	29	- Punkt inf. dla osób uzależnionych
	30	- Obrona Cywilna
	32	- Audyt, Kontrola wewnętrzna

III Wykaz zbiorów danych osobowych

W Urzędzie Miejskim przetwarzane są w systemach informatycznych oraz w postaci tradycyjnej, następujące zbiory danych osobowych:

1) Urzędu Stanu Cywilnego w Bieruniu – USC
2) Ewidencja ludności i dowodów osobistych – WSO
3) Rejestr wydanych numerów porządkowych nieruchomości – GPN
4) Rejestr planów miejscowego zagospodarowania przestrzennego oraz decyzji – GPN
5) Decyzje o rozgraniczeniu – GPN
6) Decyzje dotyczące podziału nieruchomości – GPN
7) Zbiór aktów notarialnych – GPN, RZM
8) Operaty szacunkowe dotyczące obrotu nieruchomościami – GPN
9) Decyzje dotyczące przekształcenia prawa wieczystego użytkowania w prawo własności – GPN
10) Rejestr decyzji na budowę, użytkowanie obiektów i zmian sposobu ich użytkowania – GPN
11) Rejestr decyzji ustalających warunki zabudowy i zagospodarowania terenu – GPN
12) Rejestr opłat z tytułu użytkowania wieczystego i dzierżaw – GPN
13) Ewidencja działalności gospodarczej – GK
14) Ewidencja czynszów – GK
15) Ewidencja umów na wywóz śmieci – GK
16) Umowy zlecenia i umowy o dzieło – FN
17) Ewidencja podatników, podatków i opłat lokalnych – FN
18) Tytuły wykonawcze – FN
19) Rejestr upomnień – FN
20) Rejestr zaświadczeń – FN
21) Rejestr skarg i wniosków zgłoszonych w Urzędzie Miejskim w Bieruniu – BRMiB
22) Rejestr pism do Przewodniczącego Rady Miejskiej – BRMiB
23) Ewidencja mandatów – SM
24) Ewidencja wniosków do Sądu – SM
25) Ewidencja ujawnionych wykroczeń – SM
26) Ewidencja tytułów wykonawczych – SM
27) Rejestr upomnień- SM
28) Rejestr interwencji – SM
29) Rejestr dodatków mieszkaniowych oraz najemców lokali mieszkalnych i użytkowych – GK
30) Rejestr zezwoleń sprzedaży napojów alkoholowych oraz punktów sprzedaży z napojami alkoholowymi – GK
31) Ewidencja grobów na cmentarzu komunalnym w Bieruniu, ewidencja przechowywania zwłok w domu przedpogrzebowym przy ul. Krakowskiej, ewidencja przechowywania zwłok w domu przedpogrzebowym przy ul. Soleckiej – GK
32) Rejestr decyzji o pozwolenie na wycinkę drzew - OSRiL

IV Struktura zbiorów i systemy przetwarzania

IV.1 Zbiór danych osobowych Urzędu Stanu Cywilnego w Bieruniu

IV.1.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu PB_USC oraz APUSC służącego do przesyłania danych do GUS.

IV.1.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Imiona rodziców
- Data urodzenia
- Miejsce urodzenia
- Adres zamieszkania – pobytu
- Miejsce pracy
- Zawód
- Wykształcenie
- Seria i numer dowodu osobistego
- Numer telefonu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Nazwisko rodowe matki,
- Obywatelstwo
- Stan rodzinny (imiona, nazwiska i daty urodzenia dzieci)

IV.2 Zbiór ewidencja ludności i dowodów osobistych

IV.2.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu SELWIN

IV.2.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Imiona rodziców
- Data urodzenia
- Miejsce urodzenia

- Adres zamieszkania – pobytu
- Miejsce pracy
- Zawód
- Wykształcenie
- Seria i numer dowodu osobistego
- Numer telefonu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Nazwisko rodowe matki,
- Obywatelstwo
- Stan rodzinny (imiona, nazwiska i daty urodzenia dzieci)

IV.3 Rejestr wydanych numerów porządkowych nieruchomości

IV.3.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.3.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działek

IV.4 Rejestr planów miejscowego zagospodarowania przestrzennego oraz decyzji

IV.4.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.4.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działek

IV.5 Zbiór decyzji o rozgraniczeniu nieruchomości

IV.5.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.5.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działek

IV.6 Decyzje dotyczące podziału nieruchomości

IV.6.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.6.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działek

IV.7 Zbiór aktów notarialnych

IV.7.a Forma przetwarzania:

- dokumenty papierowe

IV.7.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Imiona rodziców
- Adres zamieszkania – pobytu
- PESEL
- NIP
- Seria i numer dowodu osobistego
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działek

IV.8 Operaty szacunkowe dotyczące obrotu nieruchomościami

IV.8.a Forma przetwarzania:

- dokumenty papierowe

IV.8.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Imiona rodziców
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działki

IV.9 Decyzje dotyczące przekształcenia prawa wieczystego użytkowania w prawo własności

IV.9.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.9.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działki

IV.10 Rejestr decyzji na budowę, użytkowanie obiektów i zmian sposobu ich użytkowania

IV.10.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.10.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działki

IV.11 Rejestr decyzji ustalających warunki zabudowy i zagospodarowania terenu

IV.11.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.11.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działki

IV.12 Rejestr opłat z tytułu użytkowania wieczystego i dzierżaw

IV.12.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan i modułu Dzierżawy systemu FK

IV.12.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer działek

IV.13 Ewidencja działalności gospodarczej

IV.13.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu Ewidencja Działalności Gospodarczej

IV.13.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- PESEL
- NIP
- Miejsce pracy
- Numer telefonu

IV.14 Ewidencja czynszów

IV.14.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu aplikacji Czynsze

IV.14.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu

IV.15 Ewidencja umów na wywóz śmieci

IV.15.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu aplikacji EKOKOSZ firmy GEOBID

IV.15.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adresy zamieszkania
- NIP
- REGON

- Numery rejestracyjne pojazdów

IV.16 Umowy zlecenia i umowy o dzieło

IV.16.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu FK firmy Rekord

IV.16.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu
- PESEL
- NIP

IV.17 Ewidencja podatników, podatków i opłat lokalowych

IV.17.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu FK firmy Rekord

IV.17.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- PESEL
- NIP
- Numer telefonu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Numer rejestracyjny pojazdu

IV.18 Tytuły wykonawcze

IV.18.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu aplikacji IPS

IV.18.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania
- NIP
- PESEL

IV.19 Rejestr upomnień

IV.19.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu FK firmy Rekord

IV.19.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu

IV.20 Rejestr zaświadczeń

IV.20.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu FK firmy Rekord

IV.20.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Powierzchnia gospodarstwa rolnego

IV.21 Rejestr skarg i wniosków zgłoszonych w UM Bieruń

IV.21.a Forma przetwarzania:

- dokumenty papierowe

IV.21.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- PESEL
- Seria i numer dowodu osobistego
- Numer telefonu
- Inne

IV.22 Rejestr pism do Przewodniczącego Rady Miejskiej

IV.22.a Forma przetwarzania:

- dokumenty papierowe

IV.22.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania

IV.23 Ewidencja mandatów

IV.23.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan oraz CEPIK

IV.23.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Adres zamieszkania – pobytu
- PESEL
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Właściciel pojazdu
- Numer mandatu

IV.24 Ewidencja wniosków do Sądu

IV.24.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.24.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu
- PESEL
- Numer dowodu osobistego
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Właściciel pojazdu

IV.25 Ewidencja ujawnionych wykroczeń

IV.25.a Forma przetwarzania:

- dokumenty papierowe

IV.25.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia

- Adres zamieszkania – pobytu
- PESEL
- Numer dowodu osobistego
- I System obiegu dokumentówInne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Właściciel pojazdu

IV.26 Ewidencja tytułów wykonawczych

IV.26.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.26.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu
- PESEL
- Numer dowodu osobistego
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Właściciel pojazdu

IV.27 Rejestr upomnień

IV.27.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.27.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu

- PESEL
- Numer dowodu osobistego
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Właściciel pojazdu

IV.28 Rejestr interwencji

IV.28.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.28.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu
- PESEL
- Numer dowodu osobistego
- Inne

Inne dane osobowe, oprócz wymienionych powyżej, przetwarzane w zbiorze:

- Właściciel pojazdu

IV.29 Rejestr dodatków mieszkaniowych oraz najemców lokali mieszkalnych i użytkowych

IV.29.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.29.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu

- Numer dowodu osobistego

IV.30 Rejestr zezwoleń sprzedaży napojów alkoholowych oraz punktów sprzedaży z napojami /nieujawniony w trakcie audytu/

IV.30.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.30.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu
- Numer dowodu osobistego
- PESEL
- NIP

IV.31 Ewidencja grobów na cmentarzu komunalnym w Bieruniu, ewidencja przechowywania zwłok w domu przedpogrzebowym przy ul. Krakowskiej, ewidencja przechowywania zwłok w domu przedpogrzebowym przy ul. Soleckiej /nieujawniony w trakcie audytu/

IV.31.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.31.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu
- Numer dowodu osobistego
- PESEL
- NIP
- .....

IV.32 Rejestr pozwoleń na wycinkę drzew /nieujawniony w trakcie audytu/

IV.32.a Forma przetwarzania:

- dokumenty papierowe

- dokumenty elektroniczne przy użyciu systemu MS WORD oraz w Systemie Obiegu Dokumentów Office Objects DocMan

IV.32.b Zakres przetwarzania

Dane osobowe:

- Nazwiska i imiona
- Data urodzenia
- Adres zamieszkania – pobytu
- Numer dowodu osobistego
- PESEL
- NIP

V Opis przepływu danych osobowych

W obecnej chwili w Urzędzie Miejskim są prowadzone intensywne prace wdrożeniowe, skupiające się na integracji modułów firmy Rekord /KP – FK/

1) KP ←→ FK

- Przekazywane są następujące dane osobowe dotyczące osób : imię, nazwisko, adres, dowód osobisty, NIP, PESEL, płeć, kod ubezpieczenia.
- Wyżej wymienione dane są przekazywane w formacie XML.
- Medium przekazania danych: wewnętrzna sieć komputerowa.

2) FK → Płatnik

- Przekazywane są następujące dane osobowe dotyczące osób: imię, nazwisko, adres, dowód osobisty, NIP, PESEL, płeć, obywatelstwo, kod ubezpieczenia.
- Wyżej wymienione dane są eksportowane do pliku tekstowego a następnie importowane do płatnika
- Medium przekazania danych: sieć wewnętrzna

3) FK → Home Net /System bankowy/

- Przekazywane są następujące dane osobowe dotyczące: imię, nazwisko, numer konta, kwota świadczenia.

VI Środki bezpieczeństwa

Wykaz wdrożonych środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, mające na celu zapewnienie poufności, integralności i dostępności tych danych.

VI.1 Bezpieczeństwo fizyczne

VI.1.a Dostęp do pomieszczeń

Dostęp do pomieszczeń jest ograniczony jedynie dla upoważnionych pracowników zgodnie z przyjętą procedurą:

1) klucze do pomieszczeń pobierane / zdawane są u wyznaczonego pracownika Urzędu /pracownicy Straży Miejskiej/,
2) fakt pobrania / zdania klucza odnotowuje się w kontrolce pobierania / zdawania kluczy (wpis zawiera dokładną datę, godzinę, numer pomieszczenia oraz podpis osoby pobierającej / zdającej),
3) w czasie godzin pracy pomieszczenia nadzorowane są przez pracowników upoważnionych do samodzielnego dostępu do pomieszczenia,
4) każde pomieszczenie na czas każdej nieobecności pracownika należy zamykać na klucz.

Osoby postronne, lub nieposiadające upoważnienia do dostępu do danego pomieszczenia – w tym również praktykanci i stażyści, mogą przebywać w pomieszczeniu wyłącznie w obecności pracownika posiadającego stosowne upoważnienie.

VI.1.b Bezpieczeństwo dostępu osób trzecich

W celu zapewnienia pełnej kontroli osób trzecich z firm świadczących usługi Urząd w umowie zawiera klauzule dotyczące:

1) obowiązku przeszkolenia swojego personelu przez wykonawcę z zakresu ochrony danych osobowych, oraz możliwości weryfikowania przez Urząd wiedzy i zachowań personelu zewnętrznego w tym zakresie,
2) określenia miejsc wyłączonych z dostępu dla pracowników zewnętrznych (serwerownia, kasa, archiwum, itp.),
3) każdorazowego wyznaczenia pracownika do nadzoru personelu zewnętrznego,
4) zachowania poufności wszelkich informacji o Urzędzie na czas trwania umowy oraz po jej ustaniu.

VI.1.c Izolowane obszary przyjmowania gości

Celem ograniczenia dostępu do informacji przetwarzanej w Urzędzie nie przyjmuje się gości w tych miejscach.

W sytuacji, gdy w miejscu przetwarzania odbywa się obsługa osób pracownicy zobowiązani są do zwrócenia szczególnej uwagi na prawidłowe zabezpieczenie stanowiska pracy przed możliwością naruszenia bezpieczeństwa przetwarzanych informacji poprzez:

1) Ograniczenie do niezbędnego minimum ilości dokumentów aktualnie przetwarzanych,
2) Ograniczenie możliwości niekontrolowanego dostępu do przetwarzanej informacji przez osoby nieupoważnione do informacji w postaci papierowej np.: zamknięcie teczki, odwrócenie dokumentów stroną zawierającą informacje do dołu,
3) Odwrócenie monitora tyłem do osoby postronnej lub jeśli to nie możliwe każdorazowe uruchomienie wygaszacza ekranu bądź wyłączenie monitora.

VI.1.d Praca w obszarach chronionych

W obszarze chronionym stosuje się dodatkowe środki kontroli personelu oraz stron trzecich. Do obszarów chronionych zalicza się specjalnie stworzone strefy niedostępne dla osób postronnych, tj. pomieszczenia techniczne (serwerownia, archiwum, kasa, itp.). W wyznaczonych obszarach obowiązują zasady:

1) osoby niezatrudnione w Urzędzie, a wykonujące usługi na rzecz Urzędu, powinny wiedzieć o istnieniu obszaru chronionego lub odbywającej się tam działalności w stopniu koniecznym do wykonywania ich zadań,
2) w obszarze chronionym należy unikać wykonywania pracy bez nadzoru, co pozwala na wykluczenie możliwości pomyłki lub działania w złych zamiarach,
3) puste obszary chronione są zamknięte na klucz i poddawane okresowym kontrolom (zapisy w kontrolce pobierania / zdawania kluczy),
4) personel stron trzecich wykonujący usługi pomocnicze powinien mieć dostęp do obszaru chronionego i urządzeń przetwarzania informacji wrażliwych tylko wówczas, gdy jest to konieczne a dostęp odbywa się pod nadzorem pracownika.

VI.1.e Serwerownia i pomieszczenia węzłowe

Pomieszczenia Informatyki, jako jeden z najbardziej strategicznych obszarów, zabezpieczone są od strony dostępu do samego pomieszczenia. W pomieszczeniu serwerowni oraz węzłowych znajdują się urządzenia dostępowe (switch, router), zabezpieczające (firewall) oraz zbiór wszystkich sieciowych systemów informatycznych. Ze względów bezpieczeństwa w obszarze tym stosuje się zasady ochrony:

1) wejście zabezpieczone zamkiem spełniającymi normy ISO w zakresie trwałości oraz używalności,
2) pomieszczenia znajdujące się poza strefą ograniczonego dostępu zabezpieczone są dodatkowo zamkiem szyfrowym lub na karty zbliżeniowe,
3) dokumentacje sprzętu komputerowego oraz jego konfiguracja znajdują się w zamkniętej szafie w pomieszczeniu Referatu informatyki,

4) hasła administracyjne dostępu do urządzeń aktywnych, systemów serwerowych, stacji roboczych oraz innych urządzeń wymagających logowania przechowywane są w sejfie.

VI.1.f Stosowanie urządzeń rejestrujących

Na terenie Urzędu można używać tylko sprzętu komputerowego, fotograficznego, video i sprzętu nagrywającego, będącego własnością Urzędu Miejskiego w Bieruniu.

Na użycie innego sprzętu zgodę może wydać Burmistrz.

VI.2 Ogólne środki bezpieczeństwa

VI.2.a Upoważnienia do przetwarzania danych osobowych

Każdy pracownik, przetwarzający dane osobowe posiada upoważnienie do przetwarzania danych osobowych. Upoważnienie to, *wzór w załączniku nr 1*, zawiera: Imię i Nazwisko pracownika (Stażysty, Praktykanta); termin obowiązywania upoważnienia oraz zobowiązanie pracownika do zachowania tajemnicy. Dla umów zawartych na czas określony w systemie uprawnienia zostają ograniczone i są nadawane na czas zawarcia umowy. Z chwilą przedłużenia umowy przygotowywane są nowe upoważnienia.

Nadanie upoważnienia odbywa się zgodnie z przyjętą procedurą:

1) Wydział Kadr przekazuje informację o zatrudnieniu/zwolnieniu nowego pracownika, stażysty, praktykanta Administratorowi Bezpieczeństwa Informacji,
2) Administrator Bezpieczeństwa Informacji przygotowuje upoważnienie do przetwarzania danych osobowych/odebranie upoważnienia do przetwarzania danych osobowych oraz przekazuje dokumenty Polityki Bezpieczeństwa Informacji do zapoznania się pracownikowi,
3) Pracownik potwierdza podpisem przyjęcie do stosowania zasad bezpieczeństwa oraz zobowiązuje się do zachowania tajemnicy danych oraz sposobów ich zabezpieczania,
4) upoważnienie podpisuje ADO,
5) podpisane upoważnienie rejestruje ABI poprzez dokonanie odpowiedniego wpisu w *wykazie osób upoważnionych*, stanowiącym załącznik do polityki.

Dla każdego pracownika posiadającego upoważnienie określony zostaje poziom uprawnień do systemów przetwarzania w zależności od zajmowanego stanowiska z jednoczesnym wskazaniem, czy konieczne jest odebranie dotychczasowych uprawnień – *Wzór w załączniku nr 2*.

a) Poziom uprawnień dla kierowników wydziałów i referatów określa Burmistrz,
b) Poziom uprawnień dla pozostałych pracowników określa bezpośredni przełożony.

Upoważnienia przechowuje się w kadrach oraz u Administratora Bezpieczeństwa Informacji.

W przypadku, gdy umowa zawarta była na czas nieokreślony przy jej zakończeniu następuje odebranie upoważnienia do przetwarzania, które jest przygotowywane w kadrach - Wzór w Załączniku nr 3

VI.2.b Zasada czystego biurka i czystego ekranu

Informacje pozostawione na biurkach mogą ulec zniszczeniu lub uszkodzeniu podczas wypadków (pożar, zalanie, itp.) jak też ujawnieniu poprzez wgląd osób postronnych, dlatego też wprowadzono zasady:

1) Dokumenty papierowe oraz komputerowe nośniki informacji powinny być przechowywane w zamykanych na klucz szafach i/lub innych bezpiecznych meblach, zwłaszcza poza godzinami pracy.
2) Wrażliwe lub krytyczne informacje, pieczęcie urzędowe powinny być zamknięte w kasetach pancernych lub zabezpieczanych szafach.
3) Nie zostawiać zalogowanych komputerów osobistych, terminali i drukarek. Ochrona za pomocą zamków z kluczem, haseł i innych środków.
4) Monitory powinny być tak ustawione by uniemożliwić podgląd informacji na ekranie komputera dla osób postronnych.
5) Zabezpieczenie punktów przychodzenia i wychodzenia poczty oraz pozostających bez obsługi faksów.
6) Poza godzinami pracy fotokopiarki powinny być chronione przed użyciem przez nieuprawnione osoby (przez zamknięcie pomieszczenia lub zabezpieczenie hasłem dostępu).
7) Informacje poufne lub tajne należy natychmiast po wydrukowaniu wyjąć z drukarki.

VI.2.c Wynoszenie własności

Nie wolno wynosić wyposażenia, informacji i oprogramowania na zewnątrz bez odpowiedniego upoważnienia. Będą przeprowadzane wyrywkowe kontrole w celu wykrycia wynoszenia własności bez upoważnienia.

VI.3 Postępowanie z informacją

VI.3.a Kontrola dostępu do informacji

Pracownicy Urzędu mogą udzielać następujących informacji:

a) informowanie o funkcjonujących działach oraz o zakresie ich działania,
b) informowanie o lokalizacji działów urzędu,
c) wskazywanie siedzib innych urzędów,

d) informowanie o sposobach rozpoczęcia obsługi i podstawowych dokumentach, które trzeba złożyć,
e) podawania innych informacji wynikających z ustaw.

Osobą uprawnioną do rozpowszechniania innych informacji jest Burmistrz. Pozostali pracownicy powinni odmawiać podawania informacji oraz kierować zainteresowane osoby do sekretariatu Burmistrza.

VI.3.b Inne formy wymiany informacji

Procedury i ochrona wymiany informacji głosowej, faksowej oraz wizualnej.

Informacja taka może być podsłuchana w miejscu publicznym, odtworzona z automatycznej sekretarki, przejęta przez nieuprawnione osoby z poczty głosowej, przypadkowo wysłana faksem na zły numer. Działalność Urzędu może zostać przerwana, a informacje zagrożone, jeśli urządzenia komunikacyjne zawiodą (będą przeciążone), albo zostanie przerwana łączność. Dla zabezpieczenia przekazywanej informacji wprowadza się następujące wymogi:

1) Zachowanie szczególnej ostrożności podczas prowadzenia rozmów telefonicznych, a w szczególności zakaz przekazywania informacji poufnych i danych osobowych drogą telefoniczną.
2) Zakaz prowadzenia poufnych rozmów w miejscach publicznych (restauracje, publiczne środki transportu, itp.), szeroko dostępnych biurach, pomieszczeniach o cienkich ścianach a także na korytarzach Urzędu.
3) Nie pozostawianie wiadomości zawierających treści poufne na sekretarkach automatycznych.
4) Stosowanie wymogów Instrukcji Zarządzania Systemem Informatycznym w przypadku wykorzystywania elektronicznych środków komunikacji typu poczta e-mail.

VII Postanowienia końcowe

1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania z niniejszą polityką oraz potwierdzić ten fakt wraz ze zobowiązaniem do zachowania tajemnicy.
2) Niezastosowanie się do postanowień wprowadzonej przez Administratora Danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych osobowych przez osobę upoważnioną do przetwarzania danych osobowych może zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z art. 51-52 ustawy o ochronie danych osobowych oraz art. 266 Kodeksu karnego.
3) Polityka wchodzi w życie z dniem 1 grudnia 2009.

Bieruń, data

_____
Pieczęć ADO

Upoważnienie do Przetwarzania Danych Osobowych

NR _____

Na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 (Dz.U. z 2002 r. nr 101, poz. 926 ze zm.), upoważniam/ odbieram upoważnienie:

Panią / Pana _____

do przetwarzania danych osobowych w Urzędzie Miejskim w Bieruniu

w okresie od _____ do _____ w zakresie określonym w dokumencie „Dopuszczenie do Systemu Przetwarzania Danych Osobowych".

_____
Podpis Administratora Danych Osobowych

Zobowiązanie pracownika

Oświadczam, że zapoznałam/zapoznałem się z przepisami prawa dotyczącymi ochrony danych osobowych oraz dokumentami Polityki Bezpieczeństwa Informacji wraz z Polityką Ochrony Danych Osobowych i Instrukcją Zarządzania Systemem Informatycznym wprowadzonymi w Urzędzie Miejskim w Bieruniu dnia _____ roku zarządzeniem Burmistrza numer _____.

Zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 (Dz. U z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami), również po ustaniu zatrudnienia/odwołaniu upoważnienia/upływie jego ważności, oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych.

Mam świadomość odpowiedzialności karnej wynikającej z art. 51-52 ustawy o ochronie danych osobowych, a także art. 266 Kodeksu karnego.

_____
Data i czytelny Podpis Pracownika

Bieruń, data

Nazwa komórki

Adres komórki

Odebranie / zmiana istniejących uprawnień

Nowy pracownik Urzędu: TAK / NIE

Nazwa poprzedniej komórki: _____

Dopuszczenie do Systemu Przetwarzania Danych Osobowych

Imię i Nazwisko pracownika: _____

Miejsce pracy: _____

Data rozpoczęcia pracy: _____

Data zakończenia pracy: _____

Stanowisko: _____

Dostęp do sieci Internet: TAK / NIE

Nazwa zbioru danych osobowych:
1. _____
2. _____
3. _____
4. _____

Określenie poziomu uprawnień do systemów przetwarzania danych osobowych:

Lp.	System przetwarzania	Identyfikator	Nazwa zbioru danych osobowych			
			1.	2.	3.	4.
			Poziom uprawnień *			
1.	Papierowy					
2.						
3.						
4.						
5.						
6.						

* Należy wpisać odpowiedni poziom uprawnień: *Odczyt, zapis, kierownik, użytkownik, administrator ....*

_____
data i czytelny podpis przełożonego

Numer upoważnienia: _____

_____
podpis ABI

_____
data wykonania i podpis ASI

Bieruń, data

_____
Pieczęć ADO

Odebranie upoważnienia do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 (Dz.U. z 2002 r. nr 101, poz. 926 ze zm.), odbieram:

Pani / Panu _____

- upoważnienie do przetwarzania danych osobowych w Urzędzie Miejskim w związku z _____

- uprawnienia do systemu informatycznego.

Ostatnie miejsce pracy: _____

_____
Podpis Administratora Danych Osobowych

_____
Podpis Administratora Systemu Informatycznego

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i Nazwisko	Stanowisko	Zakres upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator upoważnionego	Podpis sporządzającego
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.							

Instrukcja Zarządzania Systemem Informatycznym

Spis treści

I Wstęp

I.1 Podstawa prawna

Instrukcję Zarządzania Systemem Informatycznym, zwaną dalej instrukcją, opracowano na podstawie przepisów:

1) Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity - Dz. U. nr 101 z 2002r. poz. 926, z późn. zm.).
2) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 z 2004r., poz. 1024).

I.2 Cel i zakres instrukcji

1) Niniejsza instrukcja reguluje zasady zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych w Urzędzie Miejskim w Bieruniu, celem zabezpieczenia ich przed zagrożeniami w szczególności przed udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.
2) Zakres przedmiotowy stosowania Instrukcji obejmuje całość systemu informatycznego przeznaczonego do przetwarzania danych osobowych w urzędzie.
3) W zakresie podmiotowym instrukcja obowiązuje wszystkich użytkowników dopuszczonych do przetwarzania danych osobowych w systemie informatycznym.

II Definicje

Ilekroć w instrukcji jest mowa o:

1) *ustawie* – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 r Nr 101, poz 926 ze zm.),
2) *rozporządzeniu* – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100 z 2004 r., poz 1024),
3) *administratorze danych osobowych* – rozumie się przez to Urząd Miejski w Bieruniu reprezentowany przez Burmistrza,
4) *administratorze bezpieczeństwa informacji* – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
5) *administratorze systemu informatycznego* – rozumie się przez to Kierownika Referatu Informatyki, któremu administrator danych powierzył pełnienie obowiązków administratora systemu informatycznego,
6) *osobie upoważnionej* – rozumie się przez to osobę którą administrator danych osobowych pisemnie upoważnił do przetwarzania danych osobowych,
7) *użytkowniku* – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym,
8) *systemie informatycznym* – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole urządzeń ze sobą współpracujących, w którym pracuje co najmniej jeden komputer centralny (serwer) i urządzenia połączone są poprzez sieć komputerową,
9) *identyfikatorze użytkownika (loginie)* – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych,
10) *haśle* – rozumie się przez to ciąg znaków znany jedynie właścicielowi przydzielonego identyfikatora,
11) *routingu* – rozumie się przez to wyznaczanie trasy i wysłanie nią pakietu danych w sieci komputerowej
12) *porcie diagnostycznym* – rozumie się przez to port umożliwiający konserwację systemu w czasie rzeczywistym
13) *kanałach ukrytych* – rozumie się przez to mechanizmy zagnieżdżania dowolnych protokołów w innych.

III Określenie systemu

Przez obszar systemu objęty niniejszą instrukcją rozumie się wszelkie urządzenia techniczne niezbędne do funkcjonowania systemu informatycznego urzędu, w którym wykonywane są zadania związane z wprowadzaniem, przetwarzaniem oraz archiwizowaniem danych osobowych lub korzystaniem ze zbiorów zawierających dane osobowe oraz pomieszczenia, w których te urządzenia się znajdują. System informatyczny eksploatowany jest na komputerach podłączonych do sieci lokalnej oraz na komputerach wolnostojących (niepodłączonych do sieci teleinformatycznej).

III.1 Ogólne wymagania bezpieczeństwa

Dołączanie do systemu innych urządzeń informatycznych, nienależących do struktury sieci musi zostać zgłoszone i uzyskać zezwolenie Burmistrza oraz działać pod nadzorem Administratora Systemu Informatycznego; *Wniosek – Załącznik nr 1*.

Sposób wykonania sieci oraz zabezpieczenia pomieszczeń systemu fizycznie lub logicznie uniemożliwiają dołączenie urządzeń do nieużywanych gniazd sieci systemu, bez ingerencji Administratora Systemu Informatycznego. Dodatkowo sieć jest monitorowana pod względem dołączonych do niej urządzeń informatycznych.

Dostęp do poszczególnych obszarów systemu jest zabezpieczony za pomocą haseł według hierarchii dostępu opracowanej przez Administratora Systemu Informatycznego, sprawdzonej pod względem formalnym przez Zastępcę Administratora Bezpieczeństwa Informacji.

W szczególności zabezpieczeniom za pomocą haseł podlega:

a) dostęp do serwerów systemu,
b) dostęp do serwera internetowego,
c) dostęp do urządzeń aktywnych sieci,
d) dostęp do konfiguracji (setup) serwerów,
e) dostęp do konfiguracji (setup) stacji roboczych,
f) dostęp do systemu dla poszczególnych użytkowników i operatorów systemu,

Sposób konfiguracji serwera oraz konstrukcja aplikacji muszą być odporne na zanik zasilania energetycznego lub inne przypadkowe uszkodzenia poszczególnych stacji roboczych, w szczególności:

1) Serwery zasilane wyłącznie przez urządzenia zasilające UPS. Za prawidłowość podłączenia, monitorowanie stanu baterii i zapisywanie uwag, w *Metryce urządzenia – UPS – Załącznik nr 2,* odpowiada Administrator Systemu Informatycznego (dotyczy tylko UPS przy serwerach).
2) Konfiguracja serwerów zapewnia automatyczne bezpieczne wyłączanie serwera w wypadku zaniku zasilania energetycznego, dłuższego niż czas podtrzymania dobranego UPS. Administrator Systemu Informatycznego wpisuje uwagi w *Metryce urządzenia – Serwer – Załącznik nr 3*.
3) Konstrukcja serwera powinna zapewniać redundancyjny układ zasilania.

Administrator Systemu Informatycznego odpowiedzialny jest za prowadzenie dzienników zdarzeń systemu i systematyczne informowanie Zastępcy Administratora Bezpieczeństwa Informacji o nieprawidłowościach wykrytych w systemie. Dzienniki zdarzeń powinny zawierać informacje

o wszystkich nieprawidłowościach systemów stwierdzonych w trakcie administrowania systemami przez Administratora Systemu Informatycznego lub przekazanych przez użytkowników systemu oraz powtarzających się awariach i naruszeniach systemu.

Administrator Systemu Informatycznego odpowiedzialny jest za przetestowanie prawidłowości konfiguracji systemu oraz aplikacji użytkowych a wynik testu oraz decyzja o dopuszczeniu do użytku odnotowana w raporcie z testów.

Konfiguracja zapewnia odnotowanie w systemie faktu rozpoczęcia pracy przez każdego z użytkowników, o ile jest to możliwe technicznie (wykaz logów). Wykaz taki podlega zabezpieczeniu łącznie z danymi systemu.

Konfiguracja systemu zapewnia odnotowanie w systemie próby nieautoryzowanego dostępu (logi systemowe i oprogramowanie specjalistyczne). Wykaz odnotowanych incydentów podlega zabezpieczeniu łącznie z danymi systemu i stanowi podstawę prawną do wszczęcia postępowania wyjaśniającego.

III.2 Wprowadzenie oprogramowania do eksploatacji

Wprowadzenie do użytkowania oprogramowania dodatkowego lub zmodyfikowanego jest dopuszczone wg następującej procedury:

a) instalacji oprogramowania dokonuje Administrator Systemu Informatycznego lub pracownicy Referatu Informatyki,
b) o ile to możliwe, próbne wdrożenie nowego oprogramowania odbywa się w warunkach laboratoryjnych (stacja robocza niezależna),
c) Administrator Systemu Informatycznego dokłada wszelkich starań, aby upewnić się, że oprogramowanie nie spowoduje żadnych negatywnych skutków dla już istniejącego systemu,
d) za prawidłowe przeprowadzenie testów, zatwierdzonych przez Zastepcę Administratora Bezpieczeństwa Informacji oraz odbiór od dostawców wdrażanego oprogramowania odpowiada Administrator Systemu Informatycznego,
e) Administrator Systemu Informatycznego odpowiada za poinformowanie Użytkowników Systemu o nowej wersji oprogramowania,
f) po zakończeniu prac odnotowuje się w *Dzienniku Systemu- Załącznik nr 4* i o ile to konieczne, w *Opisie Systemu – Załącznik nr 5* wszelkie informacje dotyczące faktu wdrożenia nowego oprogramowania, a w szczególności informacji o osobach zewnętrznych uczestniczących w pracach instalacyjnych,
g) Referat Informatyki prowadzi „Listę oprogramowania dopuszczonego do użytku w systemie informatycznym Urzędu Miejskiego w Bieruniu", która jest aktualizowana przynajmniej raz w roku.

Wprowadzenie oprogramowania odbywa się w sposób zapewniający ciągłą i stabilną pracę użytkowników. W wypadku, gdy wprowadzanie oprogramowania wymaga zatrzymania pracy Systemu, można to przeprowadzić wyłącznie za zgodą Administratora Danych Osobowych.

III.3 Instalacja oprogramowania na stacjach roboczych

Oprogramowanie instalowane na stacjach roboczych oraz komputerach przenośnych odbywa się na pisemny *Wniosek Użytkownika Systemu – Załącznik nr 6*, po zatwierdzeniu przez Burmistrza. Do wykonania instalacji zatwierdzonego oprogramowania uprawniony jest Administrator Systemu Informatycznego lub pracownicy Referatu Informatyki.

Odpowiedzialność za nieautoryzowane oprogramowanie, zainstalowane na stacji roboczej lub komputerze przenośnym ponosi jego użytkownik. Referat Informatyki posiada techniczne możliwości kontroli pracy na komputerach.

III.4 Inne zmiany w systemie

Ustalenia dotyczące wprowadzenia zmian eksploatacyjnych stosuje się odpowiednio w sytuacjach określonych poniżej, z uwzględnieniem dodatkowych szczególnych zasad:

Wprowadzanie istotnych zmian do konfiguracji systemu wymaga procedury analogicznej do obowiązującej przy wprowadzaniu oprogramowania i dotyczy:

- zmian ilości stacji roboczych,
- zmian w sposobie użytkowania serwera (w tym zmian konfiguracyjnych),
- zmian w topologii sieci.

W wypadku, gdy z dowolnego urządzenia systemu został wymontowany nośnik zawierający dane systemu, a przeznaczony:

a) do użycia,
b) zmagazynowania poza systemem,
c) likwidacji,

Administrator Systemu Informatycznego zobowiązany jest dane z nośnika usunąć w sposób trwały (poprzez zastosowanie dowolnego programu przeznaczonego do tego celu), uniemożliwiający ich odtworzenie, oraz dokonać odpowiedniej adnotacji w *Wykazie Nośników Zawierających Dane Systemu, które podległy Zbyciu – Załącznik nr 7* lub w *Wykazie Nośników Zawierających Dane Systemu, które podległy Likwidacji – Załącznik nr 8.* Nośniki zawierające kopie zabezpieczające Systemu nie mogą być używane ani magazynowane poza systemem; mogą one, co najwyżej podlegać likwidacji.

IV Uprawnienia do systemu informatycznego

IV.1 Odpowiedzialność za nadanie uprawnień

1) Kierownik komórki organizacyjnej lub bezpośredni przełożony określa zakres uprawnień.
2) Administrator Bezpieczeństwa Informacji weryfikuje oraz zatwierdza zakres uprawnień.
3) Administrator Systemu Informatycznego wykonuje czynności w Systemie Informatycznym.

IV.2 Nadawanie uprawnień do przetwarzania danych osobowych

1) Bezpośredni przełożony użytkownika występuje do Administratora Bezpieczeństwa Informacji o:
   a) założenie konta w Systemie Informatycznym, jeżeli pracownik jeszcze takiego konta nie posiada,
   b) przyznanie uprawnień w systemach informatycznych wraz z podaniem zakresu uprawnień dla osób przetwarzających dane osobowe.
2) Zastępca Administratora Bezpieczeństwa Informacji sprawdza czy użytkownik spełnia warunki dopuszczenia do przetwarzania danej grupy informacji, a w szczególności:
   a) czy użytkownik posiada upoważnienie do przetwarzania danych osobowych,
   b) czy użytkownik przeszedł szkolenie z zakresu bezpieczeństwa informacji, w tym ochrony danych osobowych,
   c) czy stanowisko pracy użytkownika, spełnia warunki dopuszczenia do przetwarzania danych osobowych,
   d) czy użytkownik podpisał oświadczenie – zobowiązanie pracownika stanowiące załącznik 1 do Polityki Bezpieczeństwa Danych Osobowych.

   Jeżeli któryś z warunków nie jest spełniony Administrator Bezpieczeństwa Informacji w porozumieniu z kierownikiem komórki organizacyjnej ustala sposób i termin uzupełnienia braków, o których mowa w rozdziale IV.2 pkt. 2).
3) Jeżeli użytkownik i jego stanowisko pracy spełniają warunki dopuszczenia, Zastępca Administratora Bezpieczeństwa Informacji przekazuje wniosek do Administratora Systemu Informatycznego o założenie konta w systemie.
4) Administrator Systemu Informatycznego przydziela identyfikator oraz przyznaje uprawnienia zgodnie z zakresem określonym w „Dopuszczeniu do systemu"
5) Administrator Systemu Informatycznego rejestruje wykonane czynności w dziennikach systemu przetwarzania.
6) Identyfikatory użytkowników posiadających uprawnienia administracyjne przyznawane są przez Burmistrza (Administratora Danych Osobowych) na wniosek Administratora Bezpieczeństwa Informacji.

IV.3 Zawieszenie uprawnień do systemu

1) W celu zapewnienia wysokiego poziomu bezpieczeństwa, bezpośredni przełożony użytkownika występuje z wnioskiem do Administratora Systemu Informatycznego o założenie blokady konta systemowego dla konkretnego pracownika w przypadku:

a) planowanej nieobecności w pracy powyżej 3 miesięcy (np.: z powodu urlopu macierzyńskiego, wychowawczego). Wniosek przygotowywany jest przed rozpoczęciem nieobecności,
b) w wypadku przedłużającej się nieobecności (np.: z powodu choroby) wniosek przygotowany jest w chwili przedłużenia nieobecności ponad 3 miesiące od chwili jej rozpoczęcia.

2) Wniosek taki powinien być złożony w formie pisemnej i powinien zawierać Imię i nazwisko pracownika, informację, od kiedy konto ma zostać zablokowane oraz powód założenia blokady konta – Załącznik nr 9.
3) Po powrocie konkretnego pracownika bezpośredni przełożony występuje w formie pisemnej do Administratora Systemu Informatycznego z wnioskiem o zdjęcie blokady.

V Uwierzytelnianie w systemie

V.1 Metody i środki uwierzytelniania

W systemie informatycznym służącym do przetwarzania danych osobowych stosowane jest uwierzytelnienie użytkownika przy pomocy jego identyfikatora oraz hasła.

V.2 Zarządzanie hasłami

1) Wszystkie hasła występujące w systemie i związane z eksploatacją podlegają okresowej zmianie zgodnie z Rozporządzeniem MSWiA.
2) Użytkowane hasła są zgodne z Rozporządzeniem MSWiA:
   a) minimalna długość hasła wynosi 8 (osiem) znaków,
   b) hasło zawiera małe i duże litery, cyfry oraz znaki specjalne,
   c) nie stanowi słowa słownikowego lub ciągu tych samych znaków,
   d) nie zawiera całości lub części loginu,
   e) zmiana hasła następuje nie rzadziej, niż co 30 dni,
   f) cykl zmian haseł nie krótszy niż 6 kolejnych zmian,
3) Treść hasła nie powinna umożliwiać identyfikacji użytkownika systemu i musi być tajna dla innych osób.
4) Ustalone hasła administracyjne są zdeponowane w zalakowanej kopercie w kasie pancernej pomieszczenia bezpieczeństwa systemu przez Administratora Systemu Informatycznego.

V.3 Zarządzanie i użytkowanie środków uwierzytelniania

1) Każdy użytkownik systemu informatycznego posiada swój unikalny identyfikator.
2) Przy tworzeniu identyfikatora użytkownika administrator systemu ustawia losowe hasło i przekazuje je w formie pisemnej użytkownikowi.
3) Użytkownik jest zobowiązany zmienić hasło, przy pierwszym dostępie do systemu.
4) Użytkownicy nie mogą używać tych samych identyfikatorów, wymieniać się identyfikatorami ani udostępniać konta komukolwiek innemu.
5) Każdy użytkownik zarządza swoimi hasłami oraz samodzielnie je zabezpiecza.
6) Użytkownicy są zobowiązani do przestrzegania reguł odnośnie długości i złożoności hasła oraz okresu jego wymiany opisanych w punkcie V.2.
7) Hasło użytkownika jest jego własnością i zna je wyłącznie dany użytkownik. Zabronione jest przekazywania hasła innym osobom.
8) Dla identyfikatorów krytycznych, którymi są identyfikatory: administratorów, managerów bezpieczeństwa oraz supervisorów dla działania danego systemu, hasło jest składowane w zaklejonej kopercie w sejfie. Tak składowane hasło może być wykorzystywane w sytuacjach kryzysowych wyłącznie przez Administratora Bezpieczeństwa Informacji lub Zastępcę Administratora Bezpieczeństwa Informacji, po poinformowaniu Administratora Danych Osobowych.

9) Hasło użytkownika jest składowane w systemie przetwarzania w sposób bezpieczny poprzez zaszyfrowanie uniemożliwiające odczytanie hasła przez użytkowników.
10) Hasło użytkownika nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu.

VI Praca w systemie informatycznym

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.

VI.1 Rozpoczęcie pracy na stacjach roboczych.

Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie, włączeniu zasilacza awaryjnego UPS (jeśli są zainstalowane) i komputera.

Następnie należy wprowadzić indywidualny identyfikator (login) oraz hasło w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać Administrator Systemu Informatycznego w porozumieniu z Zastępcą Administratora Bezpieczeństwa Informacji.

VI.2 Zawieszenie pracy na stacji roboczej

Ekran komputera wyposażony jest we włączający się po 10 minutach od przerwania pracy wygaszacz ekranu. Wznowienie pracy (wyświetlania) następuje dopiero po podaniu odpowiedniego hasła.

W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.

VI.3 Zakończenie pracy na stacji roboczej / notebooku

Zakończenie pracy na stacji roboczej następuje po zakończeniu wprowadzania danych zgodnie z procedurą:

1) Zakończenie pracy programu, w którym aktualnie przetwarzano dane,
2) Przeniesienie lub skopiowanie istotnych dokumentów w odpowiednie obszary serwera (np. katalog domowy użytkownika) do zabezpieczenia w kopii bezpieczeństwa,
3) Wylogowanie się użytkownika,
4) Wyłączenie komputera,
5) Wyłączenie zasilania w zasilaczu awaryjnym UPS oraz listwie zasilającej (jeśli zainstalowane),
6) W przypadku komputera typu notebook zabezpieczenie komputera w zamykanej szafie lub innym odpowiednio zabezpieczonym miejscu.

VI.4 Postępowanie z nośnikami informacji

Zabezpieczenie dokumentów, nośników komputerowych (taśm, dysków, kaset), danych wejściowych / wyjściowych oraz dokumentacji systemowej przed uszkodzeniem, kradzieżą i dostępem osób nieuprawnionych zapewniają:

1) Trwałe wykasowanie niepotrzebnej zawartości wszelkich nośników.
2) Usunięcie nośników należy przeprowadzać w sposób autoryzowany (zapisy, identyfikowalność).
3) Nośniki należy przechowywać w bezpiecznym otoczeniu, zgodnie z instrukcjami producenta.

VI.5 Pozbywanie się nośników

Niedbałe pozbywanie się nośników jest zagrożeniem, dlatego też nośniki zawierające informacje wrażliwe należy bezpiecznie przechowywać i likwidować, (spalenie lub niszczenie dokumentów papierowych, opróżnianie nośników z danych). W sposób bezpieczny należy pozbywać się następujących nośników:

a) dokumenty papierowe, w szczególności zawierające: raporty z danymi wyjściowymi, dane testowe,
b) wydruki programów;
c) nagrania głosowe lub inne;
d) kalki;
e) taśmy do drukarek jednorazowego użytku;
f) folie drukujące do faxów (jeśli takie są).

Administrator Systemu Informatycznego odpowiada za poprawne pozbycie się następujących nośników:

a) taśmy magnetyczne;
b) dyski lub kasety;
c) optyczne nośniki informacji (wszystkie ich formy, w tym nośniki, na których producenci dystrybuują oprogramowanie);
d) wszelkie nośniki zawierające dokumentację systemów.

W przypadku, gdy łatwiejsze będzie zebranie i pozbycie się razem wszystkich nośników, niż próby odseparowania nośników zawierających informacje poufne, możliwe wówczas jest zlecenie niszczenia nośników firmie niszczącej nośniki (weryfikacja firmy powinna obejmować: doświadczenia i stosowane środki zabezpieczeń).

Należy sporządzać dokumentację z pozbywania się informacji poufnych (identyfikowalność).

VII Sprzęt przetwarzający informacje.

VII.1 Kontrola dostępu do sieci i korzystanie z usług sieciowych

Niekontrolowane połączenia do usług sieciowych mogą mieć ujemny wpływ na całą organizację Urzędu. Użytkownicy powinni mieć dostęp wyłącznie do tych usług, do korzystania, z których są uprawnieni. Uprawnienia do poszczególnych systemów informatycznych nadawane są na pisemny wniosek Kierownika komórki organizacyjnej, za pośrednictwem Zastępcy Administratora Bezpieczeństwa Informacji. Administrator Systemu Informatycznego powinien prowadzić wykaz sieci i usług sieciowych, z których pozwala się korzystać użytkownikom.

Dla celów ochrony aplikacji oraz usług sieciowych wprowadza się następujące środki:

a) ograniczenie opcji wyboru w aplikacjach dla poszczególnych użytkowników;
b) ograniczenie dostępu do zasobów sieci;
c) aktywna kontrola uprawnionych dróg komunikacji poprzez zabezpieczenia, np. ściany ogniowe (firewall);
d) ograniczenie dostępu do sieci poprzez ustanowienie odrębnych domen logicznych, np. wirtualnych sieci prywatnych dla grup użytkowników w Urzędzie.

VII.1.b Identyfikacja węzłów sieci

Automatyczne łączenie się ze zdalnym komputerem może dać możliwość nieuprawnionego dostępu do aplikacji. Połączenia do komputerów zdalnych muszą być poddane weryfikacji tożsamości. Jeżeli połączenie wykorzystuje sieć pozostającą poza kontrolą instytucji należy identyfikować i weryfikować węzły sieci.

VII.1.c Ochrona zdalnego portu diagnostycznego

Wiele komputerów i systemów komunikacyjnych posiada możliwość wykonania zdalnego serwisowania. Kontroluje się dostęp do portów diagnostycznych.

VII.1.d Kontrola routingu w sieci

Sieci wspólne i rozległe, wymuszają kontrolę zasad dostępu. Kontrola jest istotna w przypadku wspólnych sieci ze stronami trzecimi.

Routing oparty jest na mechanizmach zapewniających pozytywną weryfikację adresów. Innym mechanizmem izolowania sieci jest translacja adresów sieciowych. Mechanizmy te działają na poziomie sprzętu lub oprogramowania (analiza przydatności stosowanych mechanizmów).

VII.1.e Kanały ukryte i konie trojańskie

Kanał ukryty ujawnia informacje przez często niejasne i pośrednie metody. Może zostać aktywowany przez zmianę parametru dostępnego jak również przez różne elementy systemu komputerowego lub przez wbudowanie informacji w ciąg danych. Koń trojański jest stworzony, aby zmieniał system pod kontem dostępności do niego w sposób nieuprawniony, trudno zauważalny i niekorzystny dla użytkownika.

Administrator Systemu Informatycznego nadzoruje następujące działania:

1) Zakup oprogramowania wyłącznie ze znanego i sprawdzonego źródła,

2) wykorzystywanie do pracy nad systemami kluczowymi sprawdzonego i zaufanego personelu,
3) zakaz kopiowania oraz instalowania programów przez użytkowników systemu informatycznego.

VII.2 Podłączenie do sieci Internet

Dostęp do sieci Internet przyznawany jest na podstawie zgody wydanej przez Burmistrza.

Korzystanie z sieci Internet odbywa się zgodnie z przyjętymi zasadami:

1) Korzystanie z sieci dozwolone jest wyłącznie dla celów służbowych,
2) Użytkownicy mają dostęp do większości polskich stron znajdujących się w domenach <nazwa>.pl, <nazwa>.org.pl oraz <nazwa>.gov.pl,
3) Istnieje możliwość pobierania plików typu: doc, rtf, txt (dokumenty tekstowe), xls (arkusze kalkulacyjne) oraz PDF (Acrobat Reader).

Jednocześnie zabronione jest :

a) przesyłanie lub udostępnianie w sieci Internet jakichkolwiek informacji lub danych w szczególności zawierających dane osobowe przy pomocy narzędzi typu: e-mail, ftp, WWW lub do połączeń bezpośrednich P2P (np.: torrent, direct connect),
b) przeglądanie stron o treściach pornograficznych,
c) łamanie praw autorskich lub licencyjnych poprzez pobieranie lub rozpowszechnianie plików muzycznych, filmów w dowolnej postaci (np.: mp3, wma, avi, DivX), oraz wszelkiego rodzaju oprogramowania,
d) korzystania z różnego rodzaju usług typu: chat, blog,
e) stosowania niezatwierdzonych komunikatorów internetowych,
f) korzystania z prywatnej poczty e-mail w szczególności do celów służbowych,
g) korzystania z portali społecznościowych (np.: „nasza-klasa"),
h) wykorzystywania w Internecie przydzielonych do celów służbowych loginów i haseł.

VII.3 Elektroniczna wymiana informacji

Przesyłanie danych osobowych lub innych informacji za pośrednictwem poczty elektronicznej (e-mail) jest dozwolone jedynie w uzasadnionych przypadkach z zachowaniem zasad bezpieczeństwa:

a) przesyłanie danych wyłącznie za pośrednictwem sprawdzonych adresów e-mail; należy potwierdzić tożsamość odbiorcy innymi metodami niż poczta elektroniczna (np. poprzez telefon) oraz fakt jego związku ze wskazaną instytucją,
b) można przesyłać jedynie jednostkowe dane, a nie całe bazy danych (np. w formie arkusza Excel) lub obszerne z nich wypisy,
c) przesyłane dane muszą zostać zaszyfrowane celem ochrony przed podsłuchem,
d) każdorazowo należy zarejestrować fakt przesłania danych wraz z informacją o zakresie przesyłanych danych, nadawcy, odbiorcy oraz celu przesłania informacji.

Każdorazowo należy rozważyć i jeśli to możliwe dostarczyć dane za pomocą innych środków (np. osobiście na płycie CD-ROM).

VII.4 Dopuszczenie nowego sprzętu do użycia

Nowe urządzenia systemu informatycznego powinny posiadać zatwierdzenie Zastępcy Administratora Bezpieczeństwa Informacji, autoryzujące ich cel i wykorzystanie. Administrator Systemu Informatycznego powinien każdorazowo sprawdzić sprzęt oraz oprogramowanie w celu zapewnienia, że są one kompatybilne z innymi urządzeniami systemu. Zatwierdzenie nowego sprzętu dodawanego do systemu odbywa się na podstawie *Protokołu zatwierdzenia nowego sprzętu do użycia – Załącznik nr 10*.

VII.5 Prywatne urządzenia przetwarzania informacji

Wykorzystywanie osobistych (prywatnych) urządzeń przetwarzania informacji (typu: Notebook, Palmtop) w systemie informatycznym jest zabronione.

Prywatne nośniki informacji (pendrive, płyta CD, dyskietka) mogą być użytkowane jedynie po sprawdzeniu pod względem obecności wirusów i uzyskaniu zgody Administratora Systemu Informatycznego.

VII.6 Utrzymywanie wyposażenia

Wyposażenie informatyczne należy utrzymywać we właściwym stanie. Administrator Systemu Informatycznego odpowiada za:

a) utrzymywanie sprzętu zgodnie z zaleceniami producenta (serwisowanie),
b) serwisowanie i naprawę wyłącznie przez uprawniony podmiot,
c) dokonywanie zapisów dotyczących wszystkich zaistniałych lub podejrzewanych awarii oraz wszystkich konserwacji i napraw,
d) wysyłanie wyposażenia poza siedzibę organizacji w celu konserwacji lub serwisowania bez narażania danych.

VII.7 Wynoszenie sprzętu

W przypadku potrzeby wykorzystywania sprzętu służbowego poza terenem Urzędu, bezpośredni przełożony osoby zainteresowanej występuje z pisemnym wnioskiem o zgodę na wynoszenie sprzętu do Administratora Bezpieczeństwa Informacji. Administrator Bezpieczeństwa Informacji opiniuje wniosek i przekazuje go do Administratora Danych Osobowych. Administrator Danych Osobowych wydaje ostateczną decyzję. Zainteresowany pracownik podpisuje oświadczenie o odpowiedzialności za sprzęt oraz zgromadzone dane. *Wzór Wniosku* znajduje się w *Załączniku nr 11*.

W przypadku konieczności stałego wynoszenia sprzętu poza siedzibę Urzędu, w miejscu terminy wyniesienia wpisuje się datę pierwszego wyniesienia sprzętu natomiast w miejscu planowanego zwrotu wpisuje się określenie STAŁA ZGODA.

Wniosek powinien być podpisany i dostarczony do Administratora Bezpieczeństwa Informacji przez bezpośredniego przełożonego.

Administrator Bezpieczeństwa Informacji po podpisaniu wniosku informuje Kierownika komórki organizacyjnej o swojej decyzji.

Oryginał wniosku zostaje zarchiwizowany u ABI, natomiast jego kserokopia zostaje przekazana do konkretnego referatu.

VII.8 Serwisowanie i naprawa sprzętu przetwarzającego informację.

W przypadku stwierdzenia nieprawidłowości działania sprzętu komputerowego lub jego uszkodzenia Użytkownik Systemu odpowiedzialny za dany sprzęt zgłasza ten fakt ustnie Administratorowi Systemu Informatycznego, który zobowiązany jest do zweryfikowania zgłoszonej awarii oraz podjęcia decyzji, co do dalszego trybu postępowania. W przypadku konieczności przekazania sprzętu do naprawy należy uwzględnić wytyczne dotyczące sposobu postępowania z nośnikami zawierającymi dane.

Fakt zgłoszenia awarii sprzętu jest odnotowywany przez Administratora Systemu Informatycznego w *Wykazie sprzętu do naprawy – wzór w Załączniku nr 12*.

Nośniki zawierające dane nie podlegają serwisowaniu poza siedzibą Urzędu zgodnie z podpisanymi umowami serwisowymi.

VII.9 Rozdzielenie urządzeń operacyjnych i testujących.

Należy dążyć do rozdzielenia systemów produkcyjnych, testujących i służących opracowywaniu nowych aplikacji oraz określenie zasad zmiany statusu oprogramowania z opracowywanego na zdatne do pracy, gdyż opracowywanie i testowanie mogą przysporzyć dużych problemów, np. spowodować niepożądaną modyfikację plików systemu operacyjnego i awarię. Należy również dążyć do tego, aby rozdzielić systemy robocze, testowe i opracowania nowych aplikacji.

W tym celu Administrator Systemu Informatycznego odpowiada za to, że, o ile możliwe:

a) oprogramowanie do opracowywania i testowania jest oddzielone,
b) funkcje opracowywania i testowania są rozdzielone,
c) dostępność kompilatorów, edytorów itp. narzędzi systemowych jest ograniczona,
d) stosowane są różne logowania do systemów roboczych i opracowywania,
e) osoby opracowujące oprogramowanie mają dostęp do kodów systemów roboczych sporadycznie i z hasłami jednorazowymi (wyłącznie w celu ich wykorzystania),
f) instalacja nowych wersji oprogramowania (upgrade) poprzedzona jest pełnym backupem systemu.

VII.10 Zasilanie

Zasilanie sprzętu obsługującego krytyczne aplikacje i bazy danych zabezpieczone jest poprzez UPS, które są regularnie sprawdzane (odpowiednia moc, testowanie – zapisy w dzienniku).

VIII Kopie zapasowe

VIII.1 Procedury tworzenia kopii zapasowych

1) Kopie zapasowe wykonywane są przez Administratora Systemu Informatycznego zgodnie ze schematem tworzenia kopii zapasowych oraz bezpieczeństwa stanowiącym załącznik nr 13, do niniejszej instrukcji.
2) Kopie bezpieczeństwa tworzy się, jako kopię odpowiedniej kopii zapasowej. Nośniki z kopiami bezpieczeństwa przechowywane są w szafie pancernej w pomieszczeniu innym niż serwerownia, w innej strefie pożarowej budynku. Przenoszenie nośników do wyznaczonego miejsca powierza się uprawnionym pracownikom.
3) Każdy nośnik podlega oznakowaniu oraz zaewidencjonowaniu zgodnie z przyjętymi zasadami zamieszczonymi w punkcie VIII.2 niniejszej Instrukcji.
4) Administrator Systemu Informatycznego odnotowuje fakt wykonania kopii zapasowej w dzienniku administratora systemu.

VIII.2 Zasady oznaczania i ewidencjonowania kopii zapasowych

Każdy nośnik, na którym wykonuje się kopie zabezpieczające, jest oznakowany w sposób trwały, zgodnie z rozporządzeniem.

Po wykonaniu kopii nośnik i obudowa (pudełko), zostają opisane zgodnie z przyjętym schematem: **NazwaSystemu_Rodzaj_Data_B,** gdzie:

Parametr	Opis
NazwaSystemu	jednoznacznie określa program / serwer,
Rodzaj	oznaczenie rodzaju kopii; np.: R, M, T, D; odpowiednio dla backupu rocznego, miesięcznego, tygodniowego, dziennego,
Data	data backupu w formacie: określenie dnia tygodnia typu: PN, WT dla kopii dziennych, RokMiesiącDzień dla pozostałych kopii (rocznej, miesięcznej, tygodniowej),
B	znacznik opcjonalny stosowany dla dodatkowej kopii miesięcznej przechowywanej w odległej lokalizacji, nośnik winien być przechowywany wraz z obwolutą w opakowaniu,

Ewidencja wykonywania kopii zabezpieczających:

1) Fakt wykonania każdej kopii zabezpieczającej należy potwierdzić w *Wykazie Kontrolnym Wykonywanych Kopii Zabezpieczających – Załącznik nr 14.*
2) Wykaz należy przygotować, określając w nim liczbę stron tego wykazu i opieczętowując każdą stronę pieczęcią Urzędu. W wypadku zapełnienia całego dziennika należy przygotować następny według powyższej procedury.

VIII.3 Programy i narzędzia do tworzenia kopii zapasowych

W systemie stosuje się następujące rodzaje nośników, na których wykonywane są różne rodzaje kopii zapasowych oraz bezpieczeństwa:

a) Płyty CD i DVD
b) taśmy magnetyczne,
c) dyski serwerów

d) serwery archiwizujące,

Kopie tworzone są w sposób automatyczny przy użyciu odpowiednich programów na wskazany rodzaj nośnika zgodnie z opisem zawartym w „Schemacie wykonywania kopii zapasowych i bezpieczeństwa."

VIII.4 Sposób i miejsce przechowywania nośników

Sposób i miejsce przechowywania nośników zawierających dane osobowe opisany został w „Schemacie wykonywania kopii zapasowych i bezpieczeństwa."

IX Zabezpieczenie systemu przed szkodliwym oprogramowaniem

1) Ruch w sieci komputerowej, zabezpieczony za pomocą zapory sieciowej oraz translacji adresów NAT, jest monitorowany przez Administratora Systemu Informatycznego w celu kontroli przepływu danych między siecią publiczną, a siecią wewnętrzną oraz kontroli działań w sieciach.
2) Poczta elektroniczna jest zabezpieczona przed przesyłaniem SPAM oraz oprogramowania złośliwego za pomocą filtrów poczty.
3) Na wszystkich stacjach roboczych oraz serwerach zainstalowane jest oprogramowanie antywirusowe.
4) Aktualizacje baz danych pobierane są codziennie do lokalnego repozytorium, z którego aktualizacje pobierane są przez pozostałe komputery.
5) Funkcjonowanie oprogramowania antywirusowego nadzorowane jest centralnie przez oprogramowanie konsoli zarządzającej.
6) Użytkownicy zostali przeszkoleni z zasad bezpieczeństwa danych, w ramach szkoleń, w szczególności:
   a) z zasad bezpiecznej pracy pozwalających unikać szkodliwego oprogramowania,
   b) z zasad postępowania w przypadku wykrycia, lub podejrzenia działania złośliwego oprogramowania.
7) Za politykę antywirusową odpowiedzialny jest Administrator Systemu Informatycznego.
8) Program antywirusowy i konfiguracja systemu musi zapewniać kontrolę całego systemu informatycznego:
   a) na bieżąco,
   b) przynajmniej raz dziennie, jeżeli z przyczyn technicznych nie możliwe jest jej zapewnienie na bieżąco,
   c) każdorazowo przy korzystaniu z nośników wymienialnych,
   d) po stwierdzonej przez Administratora Systemu Informatycznego, udanej próbie włamania do systemu informatycznego.
9) Po zasygnalizowaniu przez system antywirusowy wystąpienia wirusa, użytkownik systemu powinien natychmiast powiadomić o tym fakcie Administratora Systemu Informatycznego, który musi podjąć odpowiednie kroki:
   a) zidentyfikować wirus i określić obszar wystąpienia,
   b) odseparować, od całości, część systemu objętą wirusem,
   c) przystąpić do usuwania wirusa, zgodnie z wymogami stosowanego programu antywirusowego,
   d) w razie konieczności, należy ponownie wgrać system i dane systemu z ostatnich aktualnych kopii systemu, przetestować poprawność systemu i ponownie wykonać wszystkie operacje z bieżącego dnia.

X Sposób realizacji wymogów odnośnie ewidencji wpisów i udostępnień danych

Sposób realizacji ewidencji wpisów oraz udostępnień danych oraz innych wymagań, o których mowa w § 7 ust. 1 pkt. 4 rozporządzenia przedstawia tabela:

System	Pierwszy wpis[1]	Identyfikator[2]	Źródło[3]	Udostępnianie[4]	Sprzeciw[5]	Raport[6]
System Currenda	system odnotowuje automatycznie	system odnotowuje automatycznie	system pozwala na wprowadzenie wymaganych informacji	system pozwala na wprowadzenie wymaganych informacji	nie dotyczy	system pozwala na tworzenie raportów
.....	.....	.....	.....	.....	.....	.....

[1] Data pierwszego wprowadzenia danych osobowych do zbioru.

[2] Identyfikator osoby wprowadzającej te dane.

[3] Źródło danych (w przypadku pozyskania nie od osoby, której te dane dotyczą).

[4] Informacja o udostępnieniu danych osobowych.

[5] Sprzeciw dotyczący przetwarzania danych osobowych.

[6] Możliwość wydrukowania raportu.

XI Naruszenie bezpieczeństwa systemu informatycznego

XI.1 Określenie naruszenia bezpieczeństwa

W przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego w postaci:

a) naruszenia hasła dostępu bądź identyfikatora (loginu),
b) częściowego lub całkowitego braku danych,
c) częściowego lub całkowitego braku dostępu do danych,
d) braku dostępu do właściwej aplikacji,
e) zmiany wyznaczonego zakresu dostępu do serwera,
f) wykrycia lub podejrzenia obecności wirusa komputerowego,
g) zauważenia elektronicznych śladów (np. podejrzane ikony na pulpcie) próby włamania do systemy informatycznego,
h) znacznego spowolnienia działania systemu informatycznego,
i) podejrzenia kradzieży sprzętu komputerowego,
j) zauważenia śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

XI.2 Zadania użytkownika

Użytkownik obecny na miejscu zdarzenia zobowiązany jest do:

1) Natychmiastowego powiadomienia Administratora Systemu Informatycznego lub pracownika Referatu Informatyki,
2) Powiadomienia Administratora Bezpieczeństwa Informacji,
3) Do czasu przybycia na miejsce powiadomionego pracownika:
   a) jeżeli istnieje taka możliwość – niezwłocznego podjęcia czynności niezbędnych do powstrzymania niepożądanych skutków zaistniałego zdarzenia,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeżeli odnoszą się do zaistniałego przypadku,
   d) przygotować *Raport stwierdzenia naruszenia bezpieczeństwa – Załącznik nr 15*,
   e) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia powiadomionego pracownika.

XI.3 Zadania Administratora Bezpieczeństwa Informacji i jego zastępcy

a) Pojęcie czynności wyjaśniające przyczyny zaistnienia incydentu,
b) W przypadku potwierdzenia wystąpienia incydentu uzupełnienie raportu naruszenia bezpieczeństwa systemu informatycznego o ustalenia z przeprowadzonego dochodzenia oraz wnioski zmierzające do podjęcia niezbędnych działań,
c) Przedstawienie raportu Administratorowi Danych Osobowych,
d) Raz w roku przedstawienie Administratorowi Danych Osobowych pełnej analizy zarządzania Systemem Informatycznym.

XI.4 Zadania Administratora Systemu Informatycznego

Administrator Systemu Informatycznego w porozumieniu z Zastępcą Administratora Bezpieczeństwa Informacji:

1) Może podjąć decyzję o wyłączeniu systemu informatycznego lub jego części objętej zdarzeniem,
2) Przeprowadza postępowanie wyjaśniające w celu ustalenia okoliczności i przyczyn naruszenia bezpieczeństwa,
3) Podejmuje działania chroniące system przed ponownym wystąpieniem zagrożenia,
4) W przypadku konieczności odtworzenia danych z kopii zapasowych, Administrator Systemu Informatycznego zobowiązany jest do potwierdzenia, że kopia wykonana została przed wystąpieniem incydentu; dotyczy to zwłaszcza przypadków infekcji wirusowej.

XI.5 Zadania Administratora Danych Osobowych

Administrator Danych Osobowych:

1) Po zapoznaniu się z raportem podejmuje decyzję o dalszym trybie postępowania,
2) Powiadamia właściwe organy władzy,
3) Podejmuje inne, szczególne czynności zapewniające bezpieczeństwo systemu informatycznego.

Zastępca Administratora Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego zobowiązani są do informowania Administratora Danych Osobowych o wszelkich awariach systemu informatycznego, a w szczególności o przypadkach nadużyć spowodowanych przez użytkowników systemu informatycznego.

XII Procedury wykonywania przeglądów i konserwacji

1) Raz w roku – do końca marca – przeglądowi podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne.
2) Administrator Systemu Informatycznego przygotowuje, w porozumieniu z Zastępcą Administratora Bezpieczeństwa Informacji, plan przeglądu uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe oraz przedstawia go Administratorowi Danych Osobowych.
3) Przeglądowi podlega warstwa sprzętowa, systemy operacyjne oraz aplikacje, a także realizacja zabezpieczeń przez użytkowników Systemu Informatycznego.
4) Po dokonanym przeglądzie Administrator Systemu Informatycznego przygotowuje raport, a na jego podstawie informuje Administratora Danych Osobowych oraz Zastępcę Administratora Bezpieczeństwa Informacji o konieczności podjęcia właściwych działań korygujących i doskonalących.
5) Zakres przeglądu systemów informatycznych powinien obejmować co najmniej:
   a) zgodność z wymaganiami prawnymi w zakresie przetwarzania danych osobowych,
   b) sprawność warstwy sprzętowej do realizacji wszystkich funkcji niezbędnych z punktu widzenia wykonywanych działań,
   c) poprawność funkcjonowania systemu operacyjnego (m.in. analiza dzienników zdarzeń) oraz poprawność konfiguracji pod względem wydajnościowym jak i zapewnienia bezpieczeństwa,
   d) poprawność funkcjonowania aplikacji przetwarzających dane osobowe,
   e) zgodność liczby użytkowników systemu i ich uprawnień ze stanem oczekiwanym,
   f) zabezpieczenia systemu informatycznego ze względu na mogące się pojawić zagrożenia (np. brak zasilania, atak wirusowy, itp.),
   g) poprawność funkcjonowania systemu kopii zapasowych.
6) Wyniki przeglądu służą weryfikacji poprawności stosowanych zabezpieczeń i są wykorzystywane przy zmianach procedur Instrukcji Zarządzania Systemem Informatycznym.
7) Konserwacja sprzętu służącego do przetwarzania danych osobowych jest wykonywana przez firmy trzecie na podstawie umów na: wsparcie techniczne oraz na konserwacje sprzętu.
8) Umowy określają zakres prac i uprawnienia pracowników firmy trzeciej.

XIII Postanowienia końcowe

1) W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się z instrukcją przed dopuszczeniem do systemu przetwarzania z postanowieniami niniejszej instrukcji oraz złożyć stosowne oświadczenie potwierdzające znajomość jej treści i przyjęcie jej do stosowania.
3) Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikających z art. 51-52 ustawy ochronie danych osobowych.
4) Instrukcja wchodzi w życie dnia 1 grudnia 2009.

Bieruń, data

Wniosek o Zgodę na dołączenie sprzętu teletransmisyjnego

_____
Imię

_____
Nazwisko

_____
Stanowisko

Administrator Danych Osobowych
Urzędu Miejskiego w Bieruniu

Proszę o wyrażenie zgody na dołączenie do systemu informatycznego:

- Sprzętu w postaci .....
- Nr seryjny .....
- Na okres od ..... do .....
- W celu .....

Termin uruchomienia sprzętu: .....

Miejsce: .....

(Podpis)

Wyrażam zgodę: TAK/ NIE*

_____
(Data i Podpis ADO)

Uwagi Administratora Systemu Informatycznego :

_____

_____

* Niepotrzebne skreślić

Bieruń, data

Paszport urządzenia UPS

Wypełniający:		Data:
UPS nazwa:		Numer pokoju:
Numer seryjny:		ASI:
Zakup:	1. Data zakupu	
	2. Miejsce zakupu	
	3. Numer faktury	
Gwarancja:	1. Numer gwarancji	
	2. Data wygaśnięcia gwarancji	

Czynności sprawdzające i konserwacyjne	
Konserwacja	1. Data konserwacji .....
	2. Data kolejnej konserwacji .....
	3. Konserwacji dokonał .....
Konserwacja	1. Data konserwacji .....
	2. Data kolejnej konserwacji .....
	3. Konserwacji dokonał .....

Paszport serwera

Wypełniający:		Data:	
Serwer:		Numer pokoju:	
Numer seryjny:		ASI:	
Płyta główna:			
Procesor:		Uwagi:	
Pamięć ram:			
Karta sieciowa:			
Karta graficzna:			
Hdd 1:			
Hdd 2:			
Cd/ dvd:			
Upc:			
Inne:			
Monitor:			
Numer seryjny:			
Drukarka:			
Numer seryjny:			
Cd – dozwolone:			
Fdd – dozwolone:			
Numer ip:			
Mac adres:			
Plomba numer:			
Data zakupu:			
Miejsce zakupu:			
Numer faktury:			

Gwarancja:

1. Numer gwarancji .....
2. Data wygaśnięcia gwarancji .....

Konserwacja:

1. Data konserwacji .....
2. Data kolejnej konserwacji .....
3. Konserwacji dokonał .....

Oprogramowanie:

System operacyjny:		Licencja:
Zainstalowane poprawki:	1.	.....
	2.	.....
	3.	.....
	4.	.....
Zainstalowane łaty:	1.	.....
	2.	.....
	3.	.....
	4.	.....
Dopuszczone oprogramowanie:	1.	.....
	2.	.....
	3.	.....
	4.	.....

DODATKOWE ZAŁĄCZNIKI

Wydruk stanu konfiguracji na dzień wykonywanych w systemie zmian.

Data: .....

Dziennik systemu

Zatwierdzony:

Pieczęć Imię i nazwisko Administratora Bezpieczeństwa Informacji

Data: Podpis:

Wykaz kart „Dziennika systemu”

Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis
1.					11.					21.				
2.					12.					22.				
3.					13.					23.				
4.					14.					24.				
5.					15.					25.				
6.					16.					26.				
7.					17.					27.				
8.					18.					28.				
9.					19.					29.				
10.					20.					30.				

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

„Dziennik systemu"

Lp.	Osoba dokonująca wpisu	Data	Godzina	Opis zdarzenia (awaria, naruszenie bezpieczeństwa, konserwacja) i inne dotyczące danych osobowych	Uwagi
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

Opis systemu

Zatwierdzony:

Pieczęć | Imię i nazwisko Administratora Bezpieczeństwa Informacji

Data: | Podpis:

Wykaz sprzętu i oprogramowania eksploatowanego w systemie

Lp.	Rodzaj urządzenia	Oznaczenia (numery)	Podstawowa lokalizacja	Przeznaczenie	Eksploatowane oprogramowanie			Odpowiedzialny ASI
1.					Lp.	Nazwa programu	Numer licencji	
					1			
					2			
					3			
					4			
2.					Lp.	Nazwa programu	Numer licencji	
					1			
					2			
					3			
					4			
3.					Lp.	Nazwa programu	Numer licencji	
					1			
					2			
					3			
					4			
4.					Lp.	Nazwa programu	Numer licencji	
					1			
					2			
					3			
					4			
5.					Lp.	Nazwa programu	Numer licencji	
					1			
					2			
					3			
					4			
6.					Lp.	Nazwa programu	Numer licencji	
					1			
					2			
					3			
					4			
7.					Lp.	Nazwa programu	Numer licencji	

Lp.	Rodzaj urządzenia	Oznaczenia (numery)	Podstawowa lokalizacja	Przeznaczenie	Eksploatowane oprogramowanie	Odpowiedzialny ASI
					1 2 3 4	
8.					Lp. Nazwa programu Numer licencji 1 2 3 4	
9.					Lp. Nazwa programu Numer licencji 1 2 3 4	
10.					Lp. Nazwa programu Numer licencji 1 2 3 4	
11.					Lp. Nazwa programu Numer licencji 1 2 3 4	
12.					Lp. Nazwa programu Numer licencji 1 2 3 4	
13.					Lp. Nazwa programu Numer licencji 1 2 3 4	

1. Określenie danych systemu

2. Wykaz danych statystycznych i kontrolnych

Bieruń, data

Wniosek o instalację oprogramowania

_____
Imię

_____
Nazwisko

_____
Stanowisko

_____
Wydział

Administrator Systemu Informatycznego

Urzędu Miejskiego w Bieruniu

W związku z udostępnieniem przez ..... oprogramowania ..... proszę o instalację na komputerze w .....

Termin uruchomienia oprogramowania: .....

_____
(Podpis)

Wyrażam zgodę: TAK/ NIE*

(Data i Podpis ABI)

Uwagi Administratora Systemu Informatycznego :

.....
.....

_____

(Data i Podpis ASI)

Wykaz nośników zawierających dane, które podległy zbyciu

Zatwierdzony:

Pieczęć	Imię i nazwisko Administratora Bezpieczeństwa Informacji
	Data: Podpis:

Wykaz kart „Wykazu nośników zawierających dane, które podległy zbyciu"

Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis
1.					11.					21.				
2.					12.					22.				
3.					13.					23.				
4.					14.					24.				
5.					15.					25.				
6.					16.					26.				
7.					17.					27.				
8.					18.					28.				
9.					19.					29.				
10.					20.					30.				

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

„Wykaz nośników zawierających dane, które podległy zbyciu"

Lp.	Imię i nazwisko ASI dokonującego usunięcia danych z nośnika, zbycia nośnika i niniejszego wpisu	Rodzaj i numer nośnika	Usunięcie danych i likwidacja nośnika				Sposób zbycia nośnika
			Rodzaj danych	Sposób usunięcia danych	Data	Podpis	
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

Wykaz nośników zawierających dane, które podległy likwidacji

Zatwierdzony:

Pieczęć **Imię i nazwisko Administratora Bezpieczeństwa Informacji**

Data: **Podpis:**

Wykaz kart „Wykazu nośników zawierających dane, które podległy likwidacji"

Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis
1.					11.					21.				
2.					12.					22.				
3.					13.					23.				
4.					14.					24.				
5.					15.					25.				
6.					16.					26.				
7.					17.					27.				
8.					18.					28.				
9.					19.					29.				
10.					20.					30.				

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

„Wykaz nośników zawierających dane, które podległy likwidacji"

Lp.	Imię i nazwisko ASI dokonującego usunięcia danych z nośnika, zbycia nośnika i niniejszego wpisu	Rodzaj i numer nośnika	Usunięcie danych i likwidacja nośnika					Sposób zbycia nośnika
			Rodzaj danych	Sposób usunięcia danych	Sposób likwidacji nośnika	Data	Podpis	
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								
15.								

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

Bieruń, data

Wniosek o założenie/ zdjęcie* blokady konta systemowego

_____
Imię

_____
Nazwisko

_____
Stanowisko

_____
Wydział

Administrator Systemu Informatycznego
Urzędu Miejskiego w Bieruniu

Proszę o założenie / zdjęcie blokady* konta systemowego dla użytkownika:

..... od dnia .....
(imię i nazwisko)

Z powodu .....

_____
Podpis przełożonego

_____
Data wykonania

_____
Podpis ASI

* niepotrzebne skreślić

Bieruń, data

Protokół zatwierdzenia nowego sprzętu do użycia

Nazwa:

_____

Numer seryjny: _____

Data zakupu: _____

Dostawca / Numer faktury: _____

Gwarancja (okres): _____

Charakterystyka sprzętu:

_____

_____

Miejsce przeznaczenia:

_____

Potwierdzenie zgodności sprzętu z Systemem Informatycznym Urzędu:

_____

_____

Osoba odpowiedzialna za sprzęt oraz stanowisko:

_____

Decyzja / Uwagi do użytkowania sprzętu na terenie Urzędu:

_____

_____

_____

_____

_____ _____

Data zatwierdzenia Podpis ASI

Bieruń, data

Wniosek o zgodę na wynoszenie sprzętu

_____

Imię

_____

Nazwisko

_____

Stanowisko

_____

Wydział

Administrator Bezpieczeństwa Informacji

Urzędu Miejskiego w Bieruniu

Proszę o wyrażenie zgody na wynoszenie poza siedzibę Urzędu:

- Sprzętu w postaci .....
- Nr seryjny .....
- W celu .....
- Termin wyniesienia sprzętu: .....
- Planowany termin zwrotu sprzętu: .....

_____

(data i Podpis)

Oświadczam, iż biorę pełną odpowiedzialność za powierzony sprzęt ..... oraz wszelkie dane z nim zawarte w czasie posiadania w/w sprzętu poza siedzibą Urzędu.

_____

(podpis pracownika)

Wyrażam zgodę: TAK/ NIE*

_____

(Data i Podpis ABI)

* niepotrzebne skreślić

Wykaz sprzętu do naprawy

Zatwierdzony:

Pieczęć | Imię i nazwisko Administratora Bezpieczeństwa Informacji

Data: | Podpis:

Wykaz kart „Wykazu sprzętu do naprawy"

Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis
1.					11.					21.				
2.					12.					22.				
3.					13.					23.				
4.					14.					24.				
5.					15.					25.				
6.					16.					26.				
7.					17.					27.				
8.					18.					28.				
9.					19.					29.				
10.					20.					30.				

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

„Wykaz sprzętu do naprawy"

Lp.	Osoba dokonująca wpisu	Data	Godzina	Osoba zgłaszająca	Typ sprzętu/ lokalizacja	Opis uszkodzenia/ awarii	Uwagi o trybie postępowania	Data zakończenia naprawy
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

Schemat wykonywania kopii zapasowych oraz bezpieczeństwa

Nazwa	Rodzaj	Termin wykonania	Okres przechowywania kopii	Ilość kopii w cyklu	Nośnik
Dzienny	Różnicowy	Wtorek – Niedziela	7 dni	6 – kopia aktualna nadpisuje kopię z odpowiedniego dnia poprzedniego tygodnia	Biblioteka taśmowa
Tygodniowy	Pełny	Poniedziałek	5 tygodni	4 – kopia aktualna nadpisuje kopię sprzed 5 tygodni	Biblioteka taśmowa
Miesięczny	Pełny	Ostatni dzień miesiąca	13 miesięcy	12 – kopia aktualna nadpisuje kopię odpowiedniego miesiąca poprzedniego roku	Biblioteka taśmowa
Roczny	Pełny	Ostatni dzień roku	6 lat	5 - kopia aktualna nadpisuje kopię sprzed 6 lat	Biblioteka taśmowa
Dzienny Bezpieczeństwa	Kopia backupu dziennego	Wtorek – Niedziela	2 dni	2 – kopie nadpisywane naprzemiennie	Szafa pancerna w pokoju nr ...
Tygodniowy Bezpieczeństwa	Kopia backupu tygodniowego	Poniedziałek	2 tygodnie	2 – kopie nadpisywane naprzemienie	Szafa pancerna w pokoju nr ...

Zatwierdzony:

Pieczęć **Imię i nazwisko Administratora Bezpieczeństwa Informacji**

Data: **Podpis:**

Wykaz kontrolny wykonywania kopii zabezpieczających

Zatwierdzony:

Pieczęć | Imię i nazwisko Administratora Bezpieczeństwa Informacji

Data: | Podpis:

Wykaz kart „Wykazu kontrolnego wykonywania kopii zabezpieczających"

Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis	Numer karty	Wydział	Imię i nazwisko ASI	Data	Podpis
1.					11.					21.				
2.					12.					22.				
3.					13.					23.				
4.					14.					24.				
5.					15.					25.				
6.					16.					26.				
7.					17.					27.				
8.					18.					28.				
9.					19.					29.				
10.					20.					30.				

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

„Wykaz kontrolny wykonywania kopii zabezpieczających"

Lp.	Imię i nazwisko ASI	Data wpisu	Wykonanie kopii					Wykorzystanie / zniszczenie kopii	
			Rodzaj kopii	Data i czas wykonania	Rodzaj i numer nośnika	Miejsce zdeponowania	Potwierdzenie <podpis>	Data	Podpis
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									
10.									
11.									
12.									
13.									
14.									

Pieczęć	Numer karty	Data założenia wykazu	Podpis
		Data zamknięcia wykazu	Podpis

Bieruń, data

Raport stwierdzenia naruszenia bezpieczeństwa systemu

1. Data i godzina wystąpienia zdarzenia: _____
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   _____

   (imię, nazwisko, stanowisko służbowe)
3. Lokalizacja zdarzenia:

   _____

   (numer pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

   _____
   _____
   _____
   _____
   _____
5. Przyczyny wystąpienia zdarzenia:

   _____
   _____
   _____
   _____
   _____
6. Podjęte działania:

   _____
   _____
   _____
   _____
   _____
7. Postępowanie wyjaśniające:

   _____
   _____
   _____
   _____
   _____
8. Uwagi:

   _____
   _____
   _____
   _____

_____ _____

(Data sporządzenia i podpis sporządzającego) *(Podpis Administratora Bezpieczeństwa Informacji)*