PREZYDENT
MIASTA EŁKU

Zarządzenie Nr 5/2010
Prezydenta Miasta Ełku
z dnia 13 grudnia 2010 r.

w sprawie podstawowych warunków technicznych i organizacyjnych stosowanych w celu ochrony danych osobowych przetwarzanych w Urzędzie Miasta Ełku

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym Dz. U. z 2001 r. Nr 142, poz. 1591z późn. zm. w związku z art. 36 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm. oraz na podstawie § 3 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) zarządzam, co następuje:

§ 1

Wprowadzam „Politykę Bezpieczeństwa Urzędu Miasta Ełku" stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2

Wprowadzam „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Ełku" stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 3

Wyznaczam na stanowisko Administratora Bezpieczeństwa Informacji Urzędu Miasta Ełku Pana Michała Kaweckiego.

§ 4

Wyznaczam na stanowisko Administratora Systemu Informatycznego Urzędu Miasta Ełku Pana Wojciecha Lipińskiego.

§ 5

Zobowiązuję wszystkich pracowników Urzędu Miasta Ełku do przestrzegania polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

§ 6

Traci moc Zarządzenie Prezydenta Miasta Ełku Nr 27/99 z dnia 17.08.1999 r. w sprawie wykonania obowiązków wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 133 Poz. 883) oraz przepisów wykonawczych do tej ustawy, zmienione zarządzeniami Prezydenta Miasta Ełku nr 43/2003 z dnia 9 stycznia 2003 r. i nr 168/07 z dnia 11 czerwca 2007 r.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.

PREZYDENT MIASTA
Tomasz Andrzakiewicz

RADCA PRAWNY
Ewa Ortowska
RPŁ/S/146

PREZYDENT
MIASTA EŁKU

Załącznik nr 1 do Zarządzenia Prezydenta Miasta Ełku
Nr 5/2010 z dnia 13 grudnia 2010r.

Polityka bezpieczeństwa Urzędu Miasta Ełku

1. Wstęp

Prezydent Miasta Ełku, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanych w związku z wykonywaniem zadań administratora danych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m. in. takim jak:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej;
2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;
4) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;
5) celowe lub przypadkowe rozproszenie danych w internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;
6) ataki z internetu;
7) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
   - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nie schowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na portiernię),
   - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   - ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u administratora danych,
   - ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,

- niewykonywanie stosownych kopii zapasowych,
- przetwarzanie danych osobowych w celach prywatnych,
- wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

2. Postanowienia ogólne

1. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

1) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U z 2002 r. nr 101, poz. 926 ze zm.),
2) administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
3) administratorze danych – rozumie się przez to administratora danych Urzędu Miasta Ełku reprezentowanego przez Prezydenta Miasta Ełku,
4) administratorze systemu – rozumie się przez to informatyka Urzędu Miasta Ełku, któremu administrator danych powierzył pełnienie obowiązków administratora systemu,
5) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
6) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
7) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
8) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   - osoby, której dane dotyczą,
   - osoby upoważnionej do przetwarzania danych,
   - przedstawiciela, o którym mowa w art. 31a ustawy,
   - podmiotu, o którym mowa w art. 31 ustawy,
   - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
9) osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Prezydenta Miasta Ełku na piśmie,
10) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
11) przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

12) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

13) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

14) rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 100, poz. 1024),

15) sieci publicznej – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 28 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. nr 171, poz. 1800 ze zm.),

16) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 28 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. nr 171, poz. 1800 ze zm.),

17) serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

18) systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

19) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

20) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

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

2. Cel

Wdrożenie polityki bezpieczeństwa u administratora danych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym administratora danych i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.
W związku z tym, że w obu zbiorach administratora danych przetwarzane są między innymi dane wrażliwe, a system informatyczny administratora danych posiada szerokopasmowe połączenie z internetem, niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3. Zakres stosowania

1. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

2. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób

upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów i stażystów.

3. Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

Administrator danych osobowych reprezentowany przez Prezydenta Miasta Ełku realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
3) wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań i czynności i określa jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
4) zleca Sekretarzowi Miasta, by we współpracy z administratorem systemu oraz administratorem bezpieczeństwa informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator bezpieczeństwa informacji

Administrator bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
3) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych,
4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
5) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych,
6) zatwierdza wzory dokumentów (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne administratora danych,
7) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
8) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,

9) przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków osób upoważnianych do przetwarzania danych osobowych,

10) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych,

11) w porozumieniu z administratorem danych osobowych oraz Sekretarzem Miasta na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę,

12) przyjmuje informacje od pracownika zatrudnionego na stanowisku ds. kadr o nowo zatrudnianych pracownikach, ich stanowiskach i zakresie obowiązków oraz o pracownikach zwalnianych,

13) przygotowuje upoważnienie pracownika do przetwarzania danych osobowych,

14) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,

15) występuje z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego,

16) wzory ewidencji osób upoważnionych oraz wniosków o nadanie i odwołanie upoważnienia do przetwarzania danych osobowych określają załączniki nr 3, 4 i 6 do Polityki Bezpieczeństwa Urzędu Miasta Ełku.

3. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

3) na wniosek pracownika kadr przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także wyłącza konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,

6) wyrejestrowuje użytkowników na polecenie administratora danych lub pracownika kadr,

7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych,

8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora bezpieczeństwa informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,

9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,

10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii

zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,

11) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Stanowisko ds. kadr i szkoleń

Pracownik zatrudniony na stanowisku ds. kadr i szkoleń realizuje przede wszystkim następujące zadania w zakresie ochrony danych osobowych:

1) bezzwłocznie informuje administratora bezpieczeństwa informacji o wszystkich zatrudnianych pracownikach, stażystach i praktykantach, ich stanowiskach (miejscu pracy), zakresie obowiązków oraz ewentualnych zwolnieniach,
2) wnioskuje do administratora systemu o nadanie użytkownikowi identyfikatora i hasła dostępowego do systemu informatycznego oraz o wyłączenie identyfikatora w przypadku zwolnień ze stanowisk pracy.

5. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
2) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4) stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
5) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

4. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych stanowi załącznik nr 1 do niniejszej Polityki Bezpieczeństwa.

2. Zbiory danych

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych stanowi załącznik nr 2 do niniejszej Polityki Bezpieczeństwa .

3. System informatyczny

Zgodnie z art. 7 pkt 2a ustawy system informatyczny to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Pojęcie „system informatyczny" obejmuje elementy zaliczone do czterech kategorii. Są to:

1) urządzenia,
2) programy,
3) procedury przetwarzania informacji,
4) narzędzia programowe.

Urządzenie to „rodzaj mechanizmu lub zespół elementów, przyrządów służących do wykonania określonej czynności, ułatwiający pracę". Program – według znaczenia przyjmowanego w informatyce – to odpowiednio uporządkowana sekwencja instrukcji, mająca na celu wykonanie określonych zadań. Procedury przetwarzania informacji mogłyby być utożsamiane z programem, lecz wobec ich odrębnego wskazania w analizowanej definicji należy przyjąć, że są to procedury inne niż przyjęte w stosowanych w konkretnym przypadku programach. Narzędzia programowe także mieszczą się w kategorii oprogramowania.

System informatyczny administratora danych obsługiwany jest przez zespół serwerów zlokalizowany w budynku Urzędu Miasta przy ulicy Piłsudskiego 4, pokoju nr 110A. System ten ma bezpieczne połączenie z internetem. W systemie informatycznym przetwarzane są dane ze wszystkich zbiorów danych administratora danych. Poszczególne stacje robocze rozmieszczone są w budynkach przy ulicy Piłsudskiego numery 2, 4, 6 i 10 w pokojach zgodnie z wykazem zbiorów danych osobowych.

4. Ewidencje

W ramach struktury organizacyjnej administratora danych prowadzone są następujące ewidencje wchodzące w skład dokumentacji z zakresu ochrony danych osobowych:

1) administrator bezpieczeństwa informacji (lub osoba przez niego wyznaczona) prowadzi:
   - ewidencję osób upoważnionych do przetwarzania danych osobowych,
   - w rejestrze korespondencji ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom,
2) administrator systemu prowadzi przechowywaną w kasie pancernej ewidencję haseł administracyjnych do stanowisk roboczych poszczególnych użytkowników oraz ich identyfikatorów, a także ewidencje: komputerów przenośnych, nośników przenośnych oraz kluczy kryptograficznych.

5. Struktura zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania danych

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych, w zbiorach ewidencyjnych oraz poza zbiorami.

2. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerach bazodanowych.

3. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb komórek organizacyjnych Urzędu Miasta.

4. Zawartość pól informacyjnych, występujących w aplikacjach systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują administratora danych do przetwarzania danych osobowych.

5. Na żądanie administratora danych lub osoby przez niego upoważnionej, osoby upoważnione do przetwarzania danych zobowiązane są wskazać podstawy prawne określające zakres przetwarzanych przez nie danych.

6. Opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi, zawarte są w szczegółowych opisach aplikacji zastosowanych do przetwarzania tych danych.

7. Opisy wykonywane są przez administratora systemu w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego sporządzane są inne dostępne opisy struktury zbioru.

8. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych, wykonuje administrator systemu, zgodnie z relacjami występującymi w programach służących do przetwarzania danych osobowych dostarczonymi przez producenta aplikacji (oprogramowania).

9. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.

10. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. dyskietka, CD, DVD, taśma streamera, dysk wymienny, pendrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną).

6. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

1. Bezpieczeństwo osobowe

Zachowanie poufności

1. Administrator danych zatrudnia na wolne stanowiska w drodze naboru na stanowiska urzędnicze, awansu wewnętrznego bądź przeniesienia. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych

pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

3. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

Szkolenia w zakresie ochrony danych osobowych

1. Administrator bezpieczeństwa informacji uwzględnia następujący plan szkoleń:
   a. szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
   b. szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
   c. przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.
2. Tematyka szkoleń obejmuje:
   a. przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   b. sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
   c. obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
   d. odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
   e. zasady i procedury określone w polityce bezpieczeństwa.

2. Strefy bezpieczeństwa

W siedzibie administratora danych wydzielono strefę bezpieczeństwa klasy I, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tej strefy wchodzi pomieszczenie z serwerami i pokój stanowiący strefę bezpieczeństwa dostępu do tego pomieszczenia (pokoje 110 i 110A), w których mogą przebywać wyłącznie informatycy Urzędu Miasta, inne osoby upoważnione do przetwarzania tylko w towarzystwie tych pracowników, a osoby postronne w ogóle nie mają dostępu. Dostęp do tej strefy chroniony jest przez system alarmowy oraz elektroniczny system kontroli dostępu, który ewidencjonuje każdorazowe otwarcie drzwi.
W strefie bezpieczeństwa klasy II do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych.

3. Zabezpieczenie sprzętu

Ze względu na fakt, że system informatyczny administratora danych połączony jest z siecią publiczną, należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym. Wynikające z tego konsekwencje trzeba uwzględnić w instrukcji

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

1. Serwer jest zlokalizowany w odrębnym, klimatyzowanym pomieszczeniu, zamykanym drzwiami antywłamaniowymi klasy C (pokój 110A). Okno tego pomieszczenia zabezpieczone jest zewnętrzną kratą. W pokoju 110 mogą przebywać wyłącznie informatycy Urzędu Miasta, inne osoby upoważnione do przetwarzania tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu.

2. Informatycy Urzędu Miasta wskazują użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:

- ochronę nośników przenośnych – w tym także nośników danych, na których przechowywane są kopie zapasowe,
- prawidłową lokalizację komputerów.

3. Wszystkie urządzenia systemu informatycznego administratora danych, które przetwarzają dane osobowe są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).

4. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.

5. Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do przetwarzania danych prowadzona jest tylko przez jego pracowników, przede wszystkim zatrudnionych w dziale informatyki. Natomiast poważne naprawy wykonywane przez personel zewnętrzny realizowane są w siedzibie administratora danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.

6. Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych.

Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez administratora bezpieczeństwa informacji.

4. Zabezpieczenia we własnym zakresie

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1) ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
2) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;
3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
4) niepodłączania do listew podtrzymujących napięcie i gniazdek wydzielonej sieci elektrycznej dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia i przeciążenia (np. grzejniki, czajniki, wentylatory);

5) pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych;

6) kasowania po wykorzystaniu danych na dyskach przenośnych;

7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;

9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;

10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;

11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

12) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;

13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

16) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;

17) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

18) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

19) zachowania tajemnicy danych, w tym także wobec najbliższych;

20) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

21) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;

22) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

23) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu

dnia pracy;

24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza na nadzorowane całodobowo portierni (pokój nr 1, ul. Piłsudskiego 4).

5. Postępowanie z nośnikami i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

6. Wymiana danych i ich bezpieczeństwo

1. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego administratora danych.

2. Sporządzanie kopii zapasowych następuje w trybie opisanym w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora bezpieczeństwa informacji oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

4. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w internecie.

5. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w porozumieniu z administratorem bezpieczeństwa informacji. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa informacji lub pracowników działu informatyki oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

6. Administrator systemu w porozumieniu z administratorem bezpieczeństwa informacji dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

7. Należy stosować następujące sposoby kryptograficznej ochrony danych:

- przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP3-SSL – tunelowanie, szyfrowanie połączenia,
- przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznego kanału transmisji danych.

7. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu lub z jego upoważnienia inny pracownik zatrudniony na stanowisku informatyka po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek pracownika kadr, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.
W razie potrzeby, po uzyskaniu uprzedniej akceptacji administratora bezpieczeństwa informacji, administrator systemu lub z jego upoważnienia inny pracownik może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika (stażysta, praktykant).
Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora systemu po odebraniu przez administratora bezpieczeństwa informacji od osoby upoważnionej do przetwarzania danych oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła.
Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji i pracowników Biura Informatyki.

8. Kontrola dostępu do sieci

1. System informatyczny posiada szerokopasmowe połączenie z internetem. Dostęp do niego jest jednak ograniczony. Na poszczególnych stacjach roboczych można przeglądać tylko wyznaczone strony www bezpośrednio powiązane z zadaniami powierzonymi przez administratora danych, oraz wynikające z zakresu obowiązków na danym stanowisku.

2. Zabrania się pobierania z sieci publicznej jakichkolwiek plików programów oraz samowolnego instalowania ich na stacjach roboczych

3. Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.

4. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

5. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie pracownik Referatu Księgowości, upoważniony przez Prezydenta Miasta, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

9. Komputery przenośne i praca na odległość

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych.

2. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.

3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.

4. Wykorzystywanie komputerów przenośnych administratora danych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.

5. Do zdalnej pracy w systemie informatycznym dopuszcza się stosowanie tylko i wyłącznie szyfrowanych połączeń VPN.

6. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do administratora danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych.

7. Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:

- postępowania w razie nieobecności w pracy dłuższej niż 5 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji i uzgodnić z nim zwrot komputera przenośnego administratorowi danych;
- zwrotu sprzętu w razie zakończenia pracy u administratora danych.

8. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

10. Monitorowanie dostępu do systemu i jego użycia

System informatyczny administratora dzięki oprogramowaniu monitorującemu śledzi, kto, kiedy i jakie programy uruchamia na poszczególnych stacjach roboczych. Ponadto system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu,

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,

3) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,

4) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,

5) sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Odnotowanie informacji, o których mowa w pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 1-5.
Administrator systemu przeprowadza synchronizację zegarów stacji roboczych z serwerem, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez pracowników działu informatyki z konta o uprawnieniach administracyjnych.
System informatyczny administratora danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:

1) identyfikator użytkownika,

2) datę i czas zalogowania i wyłogowania się z systemu,

3) tożsamość stacji roboczej,

4) zapisy udanych i nieudanych prób dostępu do systemu,

5) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

11. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy)

1. Administrator bezpieczeństwa informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza kierownicy poszczególnych działów, są obowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

2. Administrator bezpieczeństwa informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.

3. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora bezpieczeństwa informacji i kierownika jednostki, w której usunięto dane osobowe.

4. Wzory dokumentów przewidujących powiadomienie, o którym mowa w art. 24 lub 25 ustawy, mogą być stosowane po zaakceptowaniu przez administratora bezpieczeństwa informacji.

5. Administrator bezpieczeństwa informacji przygotuje wykaz zbiorów danych (ewidencyjnych), w którym poszczególnym kategoriom danych osobowych przypisane zostaną okresy ich przechowywania. Wykaz ten zostanie sporządzony po przeanalizowaniu przepisów wyznaczających m. in. obowiązek przechowywania dokumentacji czy też okresy

przedawnienia roszczeń udokumentowanych z wykorzystaniem danych osobowych. Przed sporządzeniem takiego wykazu przygotowany zostanie wykaz przepisów, na mocy których przetwarzane są dane osobowe, na podstawie wykazów cząstkowych, sporządzonych przez poszczególne komórki organizacyjne.

12. Udostępnianie danych osobowych

Udostępnianie danych osobowych odbiorcom danych następuje po złożeniu wypełnionego wniosku, którego wzór został ustalony w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 19 listopada 2008 r. w sprawie określenia wzorów wniosków o udostępnienie danych z ewidencji ludności, zbioru PESEL oraz ewidencji wydanych i unieważnionych dowodów osobistych. Udostępnianie danych osobowych w inny sposób regulują przepisy ustaw szczególnych (np. Ustawa z dnia 6 kwietnia 1990 r. o Policji, Rozporządzenie Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. w sprawie wzoru imiennego upoważnienia funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego stanowiącego podstawę udostępnienia danych osobowych itp.)

13. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego.
Przykładowo przestępstwo można popełnić wskutek:

1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
2) niezabezpieczenia nośnika lub komputera przenośnego,
3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

7. Przeglądy polityki bezpieczeństwa i audyty systemu

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.
Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) zmian w budowie systemu informatycznego,
2) zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
3) zmian w obowiązującym prawie.

Administrator bezpieczeństwa informacji po uzgodnieniu z administratorem danych może stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji, jak i

administratora systemu.
Administrator danych, biorąc pod uwagę wnioski administratora bezpieczeństwa informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

8. Postanowienia końcowe

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. Każdej osobie upoważnionej do przetwarzania danych administrator bezpieczeństwa informacji przekazuje wyciąg z polityki bezpieczeństwa, a użytkownikom dodatkowo z instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, przygotowany z uwzględnieniem stanowiska tej osoby (obowiązków).
3. Naczelnicy wydziałów, kierownicy referatów i osoby zatrudnione na samodzielnych stanowiskach zobowiązani są do niezwłocznego przekazywania dla administratora bezpieczeństwa informacji aktualnych danych o lokalizacji miejsc przetwarzania danych osobowych.

PREZYDENT MIASTA
Tomasz [illegible]

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych.

1. Adres - ul. Piłsudskiego 2, pomieszczenia:
    1) Parter - numery pokoi: 1, 2, 3, 4, 5, 6, 7, 8, 15
2. Adres - ul. Piłsudskiego 4, pomieszczenia:
    1) Kondygnacja 0 - numery pokoi 02, 03, 04, 05, 07, 08, 09 oraz nieoznaczone numerami pomieszczenia archiwów akt osobowych Urzędu Miasta: pierwsze pomieszczenie – wejście od tyłu budynku (parkingu) Urzędu Miasta, drugie pomieszczenie – wejście przez pokój nr 03;
    2) Kondygnacja 1 - numery pokoi: 101, 102, 103, 104, 106, 110, 110a, 111, 112, 114 i 118;
    3) Kondygnacja 2 - numery pokoi: 232, 233, 234, 235, 236, 237, 238, 240, 241, 242, 242a, 244, 246, 253 i 254;
    4) Kondygnacja 3 - numery pokoi 369, 370, 371, 372, 373, 374, 377, 380.
3. Adres - ul. Piłsudskiego 6, pomieszczenia:
    1) Parter - numery pokoi: 1, 2, 3, 5, 7, 8, 9;
    2) Piętro - numery pokoi: 100, 101.
4. Adres - ul. Piłsudskiego 10, pomieszczenia:
    1) Piętro – pokój Biura współpracy z organizacjami pozarządowymi.

Załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Miasta Ełku

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zlokalizowanych w Ełku, przy ul. Piłsudskiego 2, 4, 6 i 10 w podziale na wydziały, samodzielne stanowiska i referaty Urzędu Miasta:

1. Biuro Profilaktyki i Rozwiązywania Problemów Alkoholowych i Narkomanii

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Rejestr osób kierowanych na zobowiązanie do podjęcia leczenia odwykowego drogą sądową	Edytory tekstów	Piłsudskiego 2 pokój 1, 2	Piłsudskiego 2 pokój 1, 2

2. Wydział Działalności Gospodarczej

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Rejestr zezwoleń na sprzedaż napojów alkoholowych	„Puma" Moduł Alkon	Piłsudskiego 4 pokój 246	Piłsudskiego 4 pokój 246
2)	Ewidencja krajowego drogowego przewozu osób	Ewidencja w Arkuszu Kalkulacyjnym	Piłsudskiego 4 pokój 246	Piłsudskiego 4 pokój 246
3)	Ewidencja działalności gospodarczej	„Puma" Moduł Ewidencja Podmiotów Gospodarczych	Piłsudskiego 4 pokój 246	Piłsudskiego 4 pokój 246

3. Wydział Świadczeń Rodzinnych i Funduszu Alimentacyjnego

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Świadczenia rodzinne	Świadczenia Rodzinne Sygnity	Piłsudskiego 6, pokoje 1, 2, 3, 100, 101	Piłsudskiego 6, pokoje 1, 2, 3, 100, 101

4. Straż Miejska

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Rejestr wykroczeń	Straż Miejska Tensoft Fotor - NORCOM Systemy Informatyczne	Piłsudskiego 2, pokoje 3 - 8	Piłsudskiego 2, pokoje 3 – 8

2)	Centralna Ewidencja Pojazdów i Kierowców	Klient OZZ – MSWi A	Piłsudskiego 2, pokój 15	Piłsudskiego 2, pokoje 3 – 8, 15

5. Urząd Stanu Cywilnego

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Urząd Stanu Cywilnego w Ełku	USC – Technika Gliwice – Akta osobowe	Piłsudskiego 4, pokoje 253, 254	Piłsudskiego 4, pokoje 253, 254

6. Wydział Planowania Przestrzennego i Gospodarki Nieruchomościami

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Mienie komunalne	„Puma" Moduł Nieruchomości	Piłsudskiego 4, pokoje 234, 235	Piłsudskiego 4, pokoje 234, 235

7. Wydział Edukacji

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Stypendia szkolne	Pomoc Materialna dla Uczniów - Sygnity	Piłsudskiego 4, pokoje 369, 370	Piłsudskiego 4, pokoje 369, 370

8. Wydział Finansowy

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Kontrahenci (umowy cywilno-prawne)	„Puma" Moduł Kontrachenci	Piłsudskiego 4 pokoje 02, 04, 05, 07, 08 , 09, 102, i 237	Piłsudskiego 4 pokoje 02, 04, 05, 07, 08 , 09, 102, i 237
2)	Podatnicy	„Puma" Moduł Podatki	Piłsudskiego 4 pokoje 02, 04, 05, 07, 08 , 09, 102	Piłsudskiego 4 pokoje 02, 04, 05, 07, 08 , 09, 102

9. Wydział Mienia Komunalnego

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Dodatki mieszkaniowe	Dodatki - Tensoft w trakcie przenoszenia na system „Puma"	Piłsudskiego 4, pokoje 242, 242a	Piłsudskiego 4, pokoje 242, 242a

		Moduł dodatki Mieszkaniowe		

10. Wydział Organizacyjny

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1)	Elektroniczny System Obiegu Dokumentów	e-SOD System Obiegu Dokumentów	Piłsudskiego 4, pokoje 106, 114	Piłsudskiego 4, pokoje 106, 114
2)	Ewidencja ludności i dowody osobiste	„Puma" Moduł Ewidencja Ludności, akta osobowe	Piłsudskiego 6, pokoje 5, 6, 7, 8	Piłsudskiego 6, pokoje 5, 6, 7, 8
3)	Kadry	„Puma" Moduł Kadry, edytory tekstów, akta osobowe	Piłsudskiego 4: parter – pokój 112, piwnica – pomieszczenia archiwów Urzędu Miasta	Piłsudskiego 4: parter – pokój 112
4)	Płace	„Płatnik", „Puma" Moduł Płace, edytory tekstów	Piłsudskiego 4 pokój 238	Piłsudskiego 4 pokój 238
5)	Rejestr skarg i wniosków	Edytory tekstów	Piłsudskiego 4 pokój 203	Piłsudskiego 4 pokój 203

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA EŁKU

L.p.	Imię i nazwisko	Data nadania	Data ustania	Zakres upoważnienia	Identyfikator	Podpis

Załącznik nr 4 do Polityki Bezpieczeństwa Urzędu Miasta Ełku

WNIOSEK O NADANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Ełk, dnia.....

Proszę o udzielenie upoważnienia do dostępu do danych osobowych Pani / Panu

.....

zatrudnionej/-emu na stanowisku.....

w .....

w następującym zakresie uprawnień:

.....

.....

Proszę o udzielenie upoważnienia w okresie od .....

do .....

.....
data i podpis

Załącznik nr 5 do Polityki Bezpieczeństwa Urzędu Miasta Ełku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH NR .....

Data nadania upoważnienia: .....

1. Upoważniam Panią/Pana .....
(imię i nazwisko upoważnianego)

zatrudnioną/-ego na stanowisku .....

w .....
(nazwa Wydziału / Referatu)

do dostępu do następujących danych osobowych:

– .....

– .....

– .....

(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba, lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

2. Identyfikator użytkownika: .....
(wypełnia się w przypadku, gdy dane przetwarzane są w systemie informatycznym)

3. Okres obowiązywania upoważnienia: .....

Wystawił: .....
(podpis administratora danych lub osoby reprezentującej administratora danych)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik nr 6 do Polityki Bezpieczeństwa Urzędu Miasta Ełku

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem ..... ustaje udzielone Panu:

.....

zatrudnionemu w Urzędzie Miasta Ełku na stanowisku:

.....

upoważnienie do przetwarzania danych osobowych nr .....

.....

(podpis administratora danych lub osoby reprezentującej administratora danych)

PREZYDENT
MIASTA EŁKU

Załącznik nr 2 do Zarządzenia Prezydenta Miasta Ełku
Nr 5/2010 z dnia 13 grudnia 2010r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Ełku

1. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, przez administratora danych – w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Definicje

Ilekroć w instrukcji jest mowa o:

1) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U z 2002 r. nr 101, poz. 926 ze zm.),
2) administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
3) administratorze danych – rozumie się przez to administratora danych Urzędu Miasta Ełku, reprezentowanego przez Prezydenta Miasta,
4) administratorze systemu – rozumie się przez to wyznaczonego przez administratora danych pracownika Biura Informatyki Wydziału Organizacyjnego Urzędu Miasta Ełku zwanym w dalszej części opracowania Biurem Informatyki,
5) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
6) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
7) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
8) odbiorcy danych – rozumie się przez to każdego, komu udostępniane są dane osobowe, z wyłączeniem:
   - osoby, której dane dotyczą,
   - osoby upoważnionej do przetwarzania danych,
   - przedstawiciela, o którym mowa w art. 31a ustawy,
   - podmiotu, o którym mowa w art. 31 ustawy,
   - organów państwowych lub organów samorządu terytorialnego, którym dane są

udostępniane w związku z prowadzonym postępowaniem,

9) osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez administratora danych na piśmie,

10) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

11) przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

12) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

13) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

14) rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 100, poz. 1024),

15) sieci publicznej – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. nr 73, poz. 852 ze zm.),

16) sieci telekomunikacyjnej – 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 ze zm.),

17) serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

18) systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

19) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

20) Help Desk - (z ang. - biuro pomocy) jest miejscem udzielania informacji i pomocy technicznej w rozwiązywaniu problemów z komputerami lub systemami teleinformatycznymi. System obsługiwany przez przeglądarkę internetową pod wskazanym przez Administratora Systemu adresie intranetowym,

21) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

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

3. Poziom bezpieczeństwa

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6 rozporządzenia.

4. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

Nadawanie i rejestrowanie uprawnień

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez administratora systemu na wniosek pracownika zatrudnionego na stanowisku ds. kadr.

2. Administrator systemu obowiązany jest upoważnić co najmniej jednego pracownika Biura Informatyki do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 14 dni.

3. Rejestracja użytkownika, o której mowa w pkt 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

4. Administrator systemu albo upoważniony pracownik, o którym mowa w pkt 2, przekazuje dla pracownika zatrudnionego na stanowisku ds. kadr zabezpieczony wydruk zawierający login oraz pierwsze hasło umożliwiające zalogowanie w systemie informatycznym, który został nadany użytkownikowi.

Wyrejestrowywanie uprawnień

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek pracownika zatrudnionego na stanowisku ds. kadr.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

   - zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   - usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:

   - nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   - zawieszenia w pełnieniu obowiązków służbowych.

5. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:

   - wypowiedzenie umowy o pracy,
   - wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.

6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest

rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

5. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Identyfikator

1. Identyfikator składa się z pierwszej litery imienia łączonego znakiem kropki z nazwiskiem użytkownika. W identyfikatorze pomija się polskie znaki diakrytyczne.

2. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu, za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator, odstępując od zasady określonej w pkt 1.

Hasło użytkownika

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

2. System informatyczny wymusza zmianę hasła co 21 dni; administrator bezpieczeństwa informacji może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

3. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

Hasło administratora

Hasło administratora systemu przechowywane jest w zamkniętej kopercie w sejfie, do którego ma dostęp wyłącznie administrator danych i administrator systemu.

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

- Tryb pracy na poszczególnych stacjach roboczych

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie, włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora.

2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo administratora bezpieczeństwa informacji.

3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach oraz w otwartych szafach.

4. Monitory komputerów wyposażone są we włączające się po 10 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.

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

roboczą.

6. Obowiązuje zakaz robienia kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez administratora systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.

7. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.

8. Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami administratora danych a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.

9. Przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.

10. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

11. Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak by zapobiec ich utracie.

12. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie.

13. Przed opuszczeniem pokoju należy:

- zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
- schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
- umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
- zamknąć okna.

14. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Klucz od pokoju przechowywany jest w pomieszczeniu dyżurnych Straży Miejskiej Urzędu Miasta Ełku (pokój nr 101 ul. Piłsudskiego 4).

- Tryb pracy na komputerach przenośnych

1. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.

2. Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.

3. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

4. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i

indywidualnego identyfikatora użytkownika.

5. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 21 dni.

6. Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu.

7. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

8. Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na serwerze administratora danych, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.

9. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to administratorowi systemu.

10. Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

- Obsługa sieci teleinformatycznej

  1. Obowiązuje zakaz przynoszenia i podłączania do sieci teleinformatycznej administratora danych jakichkolwiek urządzeń elektronicznych (laptopów, netbook-ów),
  2. Niedopuszczalne jest modyfikowanie konfiguracji połączeń sieciowych, konfiguracji sprzętowej komputerów i innych urządzeń biurowych.

7. Procedury tworzenia kopii zapasowych

1. W systemie informatycznym wykorzystującym technologię klient-serwer kopie zapasowe wykonuje się po stronie serwera.

2. Dostęp do kopii bezpieczeństwa mają tylko pracownicy Biura Informatyki Wydziału Organizacyjnego Urzędu Miasta Ełku.

3. Pozostałe kopie tworzy się na oddzielnych nośnikach informatycznych.

4. Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia.

Częstotliwość wykonywania kopii

Kopie zapasowe tworzy się:

1) codziennie – na koniec dnia kopię wszystkich danych, które uległy zmianie tego dnia,
2) raz w tygodniu – na koniec tygodnia kopię wszystkich aplikacji,

3) raz w miesiącu – na koniec miesiąca kopię zarówno danych, jak i aplikacji, w tym także systemu operacyjnego.

Testowanie kopii

W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz w tygodniu poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

Przechowywanie kopii

1. Kopie zapasowe przechowuje się w sejfie administratora danych. Dostęp do kopii posiada wyłącznie administrator systemu oraz administrator bezpieczeństwa informacji i upoważnieni przez nich pracownicy. Każde wydanie i przyjęcie kopii jest odnotowywane w rejestrze depozytów.

2. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Jednocześnie kopie zapasowe muszą być odpowiednio zabezpieczone fizycznie (sejf ognioodporny w zabezpieczonym pomieszczeniu).

Likwidacja nośników zawierających kopie

1. Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, pamięci przenośne można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.

2. Nośniki wielorazowego użytku nie nadające się do ponownego użycia należy zniszczyć fizycznie.

8. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Zbiory danych przechowywane są generalnie na serwerze obsługującym system informatyczny administratora danych. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonych każdemu użytkownikowi przez administratora systemu.

2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.

3. Na nośnikach, o których mowa w pkt 2 dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.

4. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.

5. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej instrukcji.

6. Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

7. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

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

1. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez administratora systemu.

2. Oprogramowanie, o którym mowa w pkt 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w pkt 2, administrator systemu nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.

4. Do obowiązków administratora systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.

5. Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

6. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym z sieci komputerowej administratora danych po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

7. Dostęp do internetu możliwy jest na wyznaczonych stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem firewall oraz systemem UTM (system wykrywający i zapobiegający włamaniom) oraz translacją adresów NAT.

10. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

System informatyczny administratora danych umożliwia automatycznie:

1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,

2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych),

3) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:

- datę pierwszego wprowadzenia danych do systemu administratora danych,
- identyfikator użytkownika wprowadzającego te dane,
- źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
- informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
- sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Odnotowanie informacji, o których mowa w pkt 3), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

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

1. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.

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

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

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

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

12. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1. Zgłaszanie awarii oraz wszelkich nieprawidłowości w działaniu urządzeń komputerowych odbywa się za pomocą systemu Help Desk, a wyjątkowych sytuacjach poprzez pocztę elektroniczną na adres it@um.elk.pl ,

2. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych przeprowadzane są – o ile to możliwe – przez pracowników Biura Informatyki pod nadzorem administratora systemu.

3. Naprawy i zmiany w systemie informatycznym administratora danych przeprowadzane przez serwisanta prowadzone są pod nadzorem administratora systemu w siedzibie administratora danych (jeśli to możliwe) lub poza siedzibą administratora danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

4. Jeśli nośnik danych (dysk, dyskietka, płyta lub inny) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce.

13. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1. Użytkownik zobowiązany jest zawiadomić administratora bezpieczeństwa informacji lub uprzednio wskazanego przez niego pracownika Biura Informatyki o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

- naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
- częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
- braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
- wykryciu wirusa komputerowego,
- zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
- znacznym spowolnieniu działania systemu informatycznego,
- podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
- zmianie położenia sprzętu komputerowego,
- zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

2. Do czasu przybycia na miejsce administratora bezpieczeństwa informacji lub wskazanego przez niego pracownika działu informatyki należy:

- o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
- przygotować opis incydentu,
- nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji lub osoby przez niego wskazanej.

3. Pracownik Biura Informatyki przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować administratora bezpieczeństwa informacji o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

4. Administrator bezpieczeństwa informacji po otrzymaniu zawiadomienia, o którym mowa w pkt 1, powinien niezwłocznie:

a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,

b) podjąć działania chroniące system przed ponownym naruszeniem,

c) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego administratora danych, a następnie niezwłocznie przekazać jego kopię administratorowi danych.

5. Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem systemu może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

6. W razie odtwarzania danych z kopii zapasowych administrator systemu obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).

7. Administrator danych po zapoznaniu się z raportem, o którym mowa w pkt 4 lit. c, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych bądź zastosowaniu środków ochrony fizycznej.

8. Administrator bezpieczeństwa informacji i administrator systemu zobowiązani są do informowania administratora danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

14. 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 zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.

3. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.

PREZYDENT MIASTA
Tomasz Andrukiewicz