INSTRUKCJA BEZPIECZNEGO KORZYSTANIA Z SYSTEMÓW INFORMATYCZNYCH

Spis treści:

Dokumenty powiązane:
Załącznik Nr 1 – upoważnienie do przetwarzania danych osobowych.
Załącznik Nr 2 – oświadczenie o zachowaniu poufności danych osobowych.
Załącznik Nr 3 – odwołanie upoważnienia do przetwarzania danych osobowych.

§1. Wprowadzenie

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem rozliczalności oraz integralności systemu informatycznego.

2. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez uświadamianie i szkolenie pracowników.

3. Zakres instrukcji zarządzania systemem informatycznym dotyczy wszystkich użytkowników systemu informatycznego oraz osoby przetwarzające dane osobowe.

Urząd Miasta i Gminy Kąty Wrocławskie
ul. Rynek, Ratusz 1
55-080 Kąty Wrocławskie

Dotyczy wszystkich pracowników
Wydanie 02
Data wydania 2009.06.26

§2. Ochrona pomieszczeń

1. Ochrona pomieszczeń ma na celu zabezpieczenie dostępu fizycznego osób nieuprawnionych do przetwarzania danych osobowych, oraz ochronę przed zagrożeniami pożarowymi.

2. W pomieszczeniach w których przetwarzane są dane osobowe, **osoby nieuprawnione do dostępu do danych osobowych mogą przebywać wyłącznie w obecności osoby zatrudnionej** w Urzędzie Miasta i Gminy w Kątach Wrocławskich i upoważnionej przez administratora danych do przetwarzania tych danych.

3. W pomieszczeniach, gdzie przebywaj ą osoby postronne, **monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane osoby.**

4. **Pomieszczenia**, w których przetwarzane są dane osobowe, na czas nieobecności w nich osób upoważnionych do przetwarzania danych, **musza być bezwzględnie zamykane** w sposób uniemożliwiający dostęp do nich osób postronnych.

5. Sposoby postępowania na wypadek pożaru:
    a. Ustalenie miejsca pożaru, drogi jego rozprzestrzeniania i zagrożenie dla osób przebywających w budynku urzędu.
    b. Powiadomienie o zaistniałym pożarze w pierwszej kolejności osoby, które są w budynku urzędu.
    c. Alarmowanie straży pożarnej (Tel. 998)
    d. Przed przyjazdem jednostki straży pożarnej należy próbować samodzielnie ugasić pożar.

§3. Zasady postępowania przy przetwarzaniu danych osobowych

1. W przypadku przyjęcia nowego pracownika do, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Burmistrz MiG (ADO - Administrator Danych Osobowych) wydaje upoważnienie do przetwarzania danych osobowych, którego treść stanowi *załącznik Nr 1.*

2. Pracownik, któremu administrator udzielił upoważnienia, jest zobowiązany do podpisania oświadczenia o zachowaniu poufności danych osobowych, którego treść stanowi *załącznik Nr 2.*

3. W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, która wpływa bezpośrednio na rodzaj i zakres przetwarzania danych, Burmistrz bezzwłocznie wydaje, bądź odwołuje upoważnienie, którego treść stanowi *załącznik Nr 3.*

4. W sytuacji wypowiedzenia umowy o pracę upoważnienie traci moc z datą wygaśnięcia umowy o pracę.

5. Wszystkie zbiory danych osobowych podlegają zgłoszeniu do GIODO. Wyjątkiem są zbiory danych wyszczególnione w Ustawie o Ochronie Danych Osobowych w Art. 43.1

6. W przypadku konieczności utworzenia nowego zbioru danych osobowych, wynikającej z obowiązków nałożonych przepisami ustawy bądź nowymi zadaniami, należy niezwłocznie powiadomić o tym administratora danych.

7. Informacja o której mowa w ust. 6 powinna zawierać:

    a. Nazwę zbioru,
    b. Podstawa prawna utworzenia zbioru,
    c. Metodę katalogowania (system komputerowy, metoda tradycyjna),
    d. Zakres danych zawartych w zbiorze (np. imię, nazwisko, PESEL),
    e. Informację o skazaniu, orzeczeniu o ukaraniu, mandatach karnych, orzeczeniach wydanych w postępowaniu administracyjnym,
    f. Sposób zbierania danych osobowych,
    g. Podmioty, którym dane osobowe będą udostępniane.

8. Ewidencję pracowników upoważnionych do przetwarzania danych prowadzi Wydział Organizacyjny oraz Wydział Spraw Obywatelskich (KADRY)

9. *Wgląd do danych osobowym mogą mieć wyłącznie właściciele danych osobowych, oraz osoby upoważnione przez administratora danych osobowych.*

10. *W innych przypadkach wymagane jest złożenie wniosku o udostępnienie danych osobowych, decyzję o udostępnieniu składa Administrator Danych Osobowych lub osoba przez niego wyznaczona.*

11. W obiegu wewnętrznym wprowadza się następującą zasadę udostępniania danych osobowych:

    a. Informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej”,
    b. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z obowiązującymi przepisami.

§4. Uprawnienia

1. Uprawnienia zostały przypisane do identyfikatora i hasła zapewniają dostęp użytkowników do różnych grup zbiorów danych osobowych – stosowane do indywidualnego zakresu upoważnienia.

2. Do obsługi systemu informatycznego (oprogramowania) oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, **mogą być dopuszczone wyłącznie osoby posiadające upoważnienie administratora danych lub osoby przez niego upoważnionej.**

3. Użytkownicy korzystający z systemu są rejestrowani i wyrejestrowywani przez administratora bezpieczeństwa informacji poprzez wpisanie lub wykreślenie z prowadzonego Rejestru Użytkowników Systemu Informatycznego Urzędu Miasta i Gminy w Kątach Wrocławskich.

4. Zmiany dotyczące pracownika, takie jak:
   a. Rozwiązanie umowy,
   b. Utrata upoważnienia do przetwarzania danych osobowych,
   c. Zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,

   Powodują wyrejestrowanie użytkownika w trybie natychmiastowym, zablokowanie identyfikatora użytkownika albo zmiana hasła.

5. **Wydział spraw obywatelskich (KADRY)** jest odpowiedzialny za zgłoszenie w/w zmian do Informatyka.

§5. Identyfikator i hasło.

1. **Identyfikator** umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.

2. Wszyscy użytkownicy korzystający z systemu informatycznego zobowiązani są do posługiwania hasłami zmienianymi co 30 dni.

3. Po raz pierwszy identyfikator i hasło przydziela administrator bezpieczeństwa informacji tj. osoba zatrudniona w Urzędzie Miasta i Gminy na stanowisku informatyka.

4. Hasła użytkownika do systemu informatycznego utrzymuje się w tajemnicy, również po upływie ich ważności.

5. Hasło powinno być złożone**, powinno zawierać minimum 8 znaków, duże i małe litery, cyfry lub znaki specjalne.**

6. **Haseł nie należy pozostawiać zapisanych w postaci jawnej.**

7. Hasło jest natychmiast zmieniane, jeżeli istnieje podejrzenie, że osoba nieupoważniona poznała hasło.

§6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1. Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na poufność danych osobowych.

2. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest wylogować się z systemu lub aktywować blokowany hasłem wygaszacz ekranu.

3. Kończąc pracę należy wyłączyć wszystkie programy, wylogować się z systemu informatycznego a następnie wyłączyć sprzęt komputerowy.

4. Należy zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne na których znajdują się dane osobowe.

§7. Kopie zapasowe

1. Za wykonywanie kopii zapasowych odpowiedzialni są Informatycy.

2. Obowiązkiem pracowników jest pozostawianie wszystkich plików wymaganych do wykonywania zadań służbowych na dyskach sieciowych.

3. Pliki przechowywane na komputerach lokalnych nie podlegają polityce kopii zapasowych.

§8. Ochrona dokumentów w formie papierowej.

1. Wykonywanie wydruków związanych z przetwarzaniem danych osobowych następuje wyłącznie w zakresie i ilości niezbędnej dla celów służbowych, uzgodnionych z przełożonym.

2. Wszelkie wydruki komputerowe zawierające dane osobowe, które nie są przeznaczone do udostępnienia, należy przechowywać w warunkach uniemożliwiających dostęp do nich osobom niepowołanym

3. Wynoszenie dokumentów poza chroniony teren urzędu jest możliwe w szczególnie uzasadnionych przypadkach za zgodą kierownika. Dokumenty wynoszone poza teren urzędu muszą podlegać szczególnej ochronie.

4. Przesyłki zawierające dane osobowe rejestruje się w prowadzonym „Dzienniku korespondencji". „Dziennik" prowadzony jest przez …… .

5. Polityka „**czystego** biurka" nakazuje nie zostawiać na wierzchu żadnych dokumentów, kiedy na pewien okres czasu tracimy kontrolę nad nimi. Niepotrzebne w danym momencie dokumenty papierowe i nośniki danych (płyty CD, DVD, pendrive'y, taśmy) należy bezwzględnie chować w zamykanych szafach.

6. Na czas remontu pomieszczeń, naprawy urządzeń i sprzętu oraz w czasie innych okoliczności zakłócających normalny tok pracy, kierownik podejmuje odpowiednie przedsięwzięcia mające na celu należyte zabezpieczenie dokumentów zawierających dane osobowe.

§9. Zasady bezpiecznej pracy w systemie komputerowym

1. W celu rozpoczęcia pracy użytkownik po uruchomieniu komputera jest zobowiązany do wpisania hasła przydzielonego mu przez administratora bezpieczeństwa informacji.
2. Udostępnienie haseł osobom trzecim jest niedopuszczalne.
3. Użytkownik jest zobowiązany do monitorowania poprawnego działania programu antywirusowego.
4. Program antywirusowy automatycznie kontroluje dostęp do wszystkich plików.
5. W przypadku przerwy w pracy należy zablokować dostęp do komputera.
6. Wyłączenie komputera następuje po uprzednim upewnieniu się, że pozostali użytkownicy nie używają zasobów używanego komputera.
7. Przed wyłączeniem komputera użytkownik jest zobowiązany do zakończenia pracy wszystkich programów.
8. Sieć Internet może być wykorzystywana wyłącznie do celów służbowych.
9. Korzystając z przeglądarki internetowe nie wolno zapamiętywać programie haseł.
10. Nie wolno używać haseł wykorzystywanych do pracy w urzędzie do logowania się na strony internetowe.
11. Przy korzystaniu z poczty elektronicznej należy zachować szczególną ostrożność przy otwieraniu załączników oraz przy korzystaniu z przysłanych linków do stron WWW.
12. Korzystanie z pamięci masowych typu pendrive jest możliwe o ile nie będą tam składowane dane osobowe oraz dokumenty narażające dobre imię urzędu w chwili wycieku.
13. Komputery przenośne należy przewozić gwarantując ich bezpieczeństwo, nie wolno pozostawiać komputera w samochodzie w widocznym miejscu, udostępniać osobom niepowołanym.
14. Postępowanie w zakresie komunikacji sieciowej, a w szczególności zasady dostępu do zasobów sieci określa administrator bezpieczeństwa informacji poprzez przydzielanie haseł dostępu do określonych zasobów.
15. Nie wolno samodzielnie modyfikować ustawień systemu oraz ingerować w konfigurację sprzętową.
16. Niedopuszczalne jest podłączanie do sieci urzędu komputerów i urządzeń sieciowych bez zgody administratora.

§10. Bezpieczeństwo oprogramowania.

1. Dopuszczalne jest korzystanie z oprogramowania zaakceptowanego przez Wydział Organizacyjny.
2. Instalacje oprogramowania dokonuje wyłącznie pracownik Wydziału Organizacyjnego.
3. Ściąganie oprogramowania z sieci Internet jest zabronione.
4. Modyfikowanie ustawień oprogramowania jest możliwe po uzgodnieniu z Wydziałem Organizacyjnym.
5. Możliwe jest posługiwania się wyłącznie programami autoryzowanymi lub zakupionymi od licencjonowanych dostawców.
6. Każdy komputer wyposażony jest w metrykę komputera. Za aktualne informację na metryce odpowiedzialny jest pracownik urzędu.

§11. Monitorowanie bezpieczeństwa Danych Osobowych

1. Kierownicy wydziałów UMiG, w których przechowywane są dane osobowe, zobowiązani są do sprawowania nadzoru nad pracownikami upoważnionymi do dostępu do danych osobowych oraz dopilnowania aby po zakończeniu pracy zabezpieczali oni należycie dostęp do danych osobowych.
2. Administrator bezpieczeństwa informacji sprawuje nadzór i kontrolę w zakresie: dbałości o wykorzystywany w pracy sprzęt komputerowy (komputery, drukarki i pozostałe urządzenia) oraz zapewnienia jego użytku wyłącznie do celów służbowych,
3. Obszar objęty monitoringiem:
    a. Ruch sieciowy
    b. Uruchamianie oprogramowania
    c. Logowanie do systemu
    d. Korzystanie z programów sieciowych

§12. Zgłaszanie incydentów bezpieczeństwa

1. Użytkownik systemu informatycznego zobowiązany jest zawiadomić administratora bezpieczeństwa informacji o każdym naruszeniu zabezpieczenia systemu polegającym w szczególności na;
    a. naruszeniu hasła dostępu (system nie reaguje na hasło lub je ignoruje- usunięty mechanizm hasła),
    b. częściowym lub całkowitym braku bazy danych,
    c. braku możliwości uruchomienia właściwej aplikacji (programu komputerowego),

d. zmianie położenia sprzętu komputerowego lub możliwości połączenia wszystkich urządzeń,
e. kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy.

2. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym jest administrator bezpieczeństwa informacji, którego zadaniem jest w szczególności przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

3. Administrator bezpieczeństwa informacji, po otrzymaniu zawiadomienia o naruszeniu zabezpieczenia systemu informatycznego powinien niezwłocznie:
   a. powiadomić administratora danych lub osobę przez niego upoważnioną.
   b. przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia i osoby odpowiedzialnej za naruszenie,
   c. podjąć działania zabezpieczające system przed ponownym naruszeniem,
   d. sporządzić protokół dokonanych czynności.
4. W przypadku kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy należy o tym fakcie niezwłocznie powiadomić Policję. Informacja o zbiorach danych osobowych i ich strukturze (w zakresie danych osobowych), programach przetwarzających dane osobowe (wg Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., D.U. Nr 100 póz. 1024 §4, pkt. 2,3,4).

§13. Postępowanie dyscyplinarne

1. W przypadku, gdy pracownik przekracza swoje uprawnienia lub nie wypełnia zapisów umowy o prace (zakres obowiązków, uprawnień i odpowiedzialności) oraz nie przestrzega zapisów Polityki Bezpieczeństwa Informacji podlega odpowiedzialności dyscyplinarnej zgodnie Kodeksem Pracy: np. upomnienie i okresowe zablokowanie dostępu – cofniecie uprawnień, nagana, zwolnienie dyscyplinarne.