Straż Miejska w Cieszynie
ul. Limanowskiego 7
43-400 CIESZYN
Tel. 33/8579 400, tel./fax 33/8579 402

Załącznik Nr 2
do Zarządzenia Nr 6/2011
Komendanta Straży Miejskiej w Cieszynie
z dnia 15 marca 2011 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM STRAŻY MIEJSKIEJ W CIESZYNIE

Cieszyn 2011

Podstawa prawna § 3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 z 2004 roku, poz. 1024).

I. Postanowienie ogólne

1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, uszczegóławia postępowanie z systemem informatycznym, w tym z aplikacjami służącymi do przetwarzania danych osobowych opisanymi w Polityce bezpieczeństwa.
2. Z Instrukcją zarządzania systemem informatycznym zobowiązani są zapoznać się wszyscy użytkownicy systemu informatycznego Komendy Straży Miejskiej w Cieszynie w zakresie niezbędnym do prawidłowego i bezpiecznego wykorzystania systemu.
3. W związku z faktem, że żadne urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną, w Komendzie Straży Miejskiej w Cieszynie stosuje się środki bezpieczeństwa danych osobowych na **poziomie podwyższonym,** zgodnie z załącznikiem do rozporządzenia MSWiA z dnia 29 kwietnia 2004r w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
4. Jako pomieszczenie szczególnie chronione wyznacza się pokój - serwerownię.
5. Kierownictwo komendy wspiera działania zmierzające do podniesienia świadomości użytkowników w zakresie przetwarzania danych osobowych, w tym bezpieczeństwa danych w systemie informatycznym.
6. Dąży się to tego, aby wszystkie zakupione urządzenia, systemy i aplikacje służące do przetwarzania danych osobowych spełniały wymogi przepisów ustawy o ochronie danych osobowych i innych przepisów mających wpływ na bezpieczeństwo przetwarzanych danych.

II. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Bezpośredni przełożony użytkownika zwraca się do Administratora Danych z pisemnym wnioskiem o nadanie uprawnień, określającym zakres dostępu do systemu informatycznego.

2. Administrator Danych w uzgodnieniu z Administratorem Bezpieczeństwa Informacji oraz Administratorem Systemu Informatycznego wyraża zgodę na nadanie uprawnień do systemu informatycznego lub odmawia nadania uprawnień z podaniem przyczyny.

3. Administrator Danych wydaje upoważnienie do przetwarzania danych osobowych zgodnie z wnioskiem.

4. Na podstawie wydanego upoważnienia Administrator Systemu Informatycznego lub wyznaczony przez niego pracownik nadaje uprawnienia w systemie informatycznym.

5. Nadanie uprawnień następuje na dwóch poziomach:

- Zarejestrowania w systemie informatycznym dla nowego użytkownika.
- Nadanie uprawnień dostępu do zasobów systemu informatycznego.

6. Odwołanie upoważnienia lub wygaśnięcie ważności upoważnienia skutkuje natychmiastowym zablokowaniem dostępu pracownikowi do określonych zasobów systemu informatycznego.

7. Bezpośredni przełożony upoważnionego pracownika powiadamia Administratora Systemu Informatycznego i Administratora Danych o odejściu z pracy użytkownika lub zmianie zakresu obowiązków mających wpływ na zakres przetwarzanych danych.

8. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelnienia lub stwierdzenia innej sytuacji naruszenia ochrony Administrator Systemu Informatycznego jest zobowiązany zablokować użytkownikowi dostęp do systemu informatycznego, powiadamiając o tym fakcie Administratora Danych.

III. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Do uwierzytelnienia w systemie używa się identyfikatora i hasła.

2. Każdorazowo uwierzytelnienie użytkownika w systemie następuje po podaniu własnego identyfikatora i hasła.

3. Dodatkowego uwierzytelnienia wymaga dostęp do aplikacji służących do przetwarzania danych osobowych.

4. Unikalny identyfikator jest nadawany przez Administratora Systemu Informatycznego lub innego wyznaczonego pracownika podczas rejestracji w systemie informatycznym.

5. Przy tworzeniu identyfikatora użytkownika Administrator Systemu Informatycznego ustawia hasło, które w sposób bezpieczny bezpośrednio przekazuje użytkownikowi.

6. Użytkownik zobowiązany jest zmienić hasło, o ile system na to pozwala, przy pierwszym dostępie do systemu.

7. Każdy użytkownik zarządza swoimi hasłami dla wszystkich identyfikatorów, których używa.

8. Hasło użytkownika jest jego własnością.

9. Zabronione jest przekazywania hasła innym osobom.

10. Zabronione jest włączanie funkcji zapamiętywania wprowadzonego hasła i loginu przez przeglądarki internetowe i inne aplikacje.

11. Hasło musi się składać z co najmniej 8 znaków, zawierając małe i wielkie litery oraz cyfry lub znaki specjalne. Za odpowiednią złożoność hasła odpowiada użytkownik.

12. Zabronione jest stosowanie cyklicznie zmienianych haseł.

13. Zabronione jest stosowanie tych samych haseł w systemach służbowych i prywatnych.

14. Zmiana hasła następuje nie rzadziej niż co 30 dni.

15. W przypadku kiedy system nie wymusza automatycznie zmiany hasła do okresowej zmiany hasła zobowiązany jest użytkownik.

16. Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych użytkowników. Jeżeli użytkownik w pobliżu zaczyna wprowadzać hasło należy odwrócić wzrok.

17. Użytkownik musi dołożyć szczególnej staranności podczas wprowadzania hasła do systemu, aby inna osoba nie miała możliwości jego podglądu.

18. Hasło użytkownika nie może być wyświetlane na ekranie w postaci otwartego tekstu.

19.Hasło użytkownika nie może być przesyłane przez sieć otwartym tekstem, przekazywane przez telefon oraz przez osoby trzecie.

20. Zabrania się zapisywania hasła w miejscach ogólnie dostępnych.

21. Hasło użytkownika jest składowane w systemie przetwarzania w bezpieczny sposób.

22. Nadzór nad hasłami przechowywanymi w systemie sprawują administratorzy systemu informatycznego.

23.Szczególnego postępowania wymagają hasła administratorów poszczególnych systemów i aplikacji.

24.Postępowania z hasłami administracyjnymi określa administrator systemu informatycznego.

25. Uprawnienia administracyjne do poszczególnych systemów mają osoby wyznaczone przez Komendanta.

26. Do każdego systemu informatycznego na prawach administratora musi mieć dostęp przynajmniej dwóch pracowników, aby wyeliminować sytuację braku możliwości administracji danym systemem w przypadku losowego wypadku.

28. W uzasadnionych przypadkach dostęp do danego systemu na prawach administratora może mieć również inny pracownik Straży Miejskiej, który posiada wystarczającą wiedzę informatyczną umożliwiającą administrowanie w sposób bezpieczny systemem służącym

do przetwarzania danych osobowych.

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

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić stanowisko pracy oraz komputer, ze szczególnym zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
a/ włączenie komputera i innych urządzeń peryferyjnych,
b/ uwierzytelnienia w systemie sieci informatycznej za pomocą identyfikatora i hasła,
c/ uwierzytelnienia w systemie aplikacyjnym.
3. Dla urządzeń komputerowych, mających odpowiednie możliwości techniczne, ekrany monitorów muszą być automatycznie wygaszane w przypadku ponad 10 minutowej nieaktywności.
Za odpowiednie ustawienie wygaszacza odpowiada użytkownik komputera.
4. Każda osoba opuszczająca stanowisko pracy – pomieszczenie musi wylogować się z aplikacji i systemu.
5. Pracę w systemach i aplikacjach należy zakończyć zgodnie z wymogami danego systemu (np. przez wybór funkcji "koniec", "wylogowanie", „zamknij") i po potwierdzeniu operacji w prawidłowy sposób wyłączyć sprzęt komputerowy.
6. Użytkownik zabezpiecza swoje stanowisko pracy, w szczególności zewnętrzne nośniki informacji, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych. Wydruki komputerowe. które nie będą już używane niszczy w sposób uniemożliwiający odtworzenie.

V. Procedury tworzenia kopii zapasowych zbiorów danych, procedury związane z ich zarządzaniem i użytkowaniem oraz sposób, miejsce i okres przechowywania elektronicznych nośników informacji i kopii zapasowych:

Elektroniczne nośniki informacji.

1. Przez elektroniczne nośniki informacji należy rozumieć wszystkie nośniki, na których przechowywane są dane w postaci elektronicznej,
2. Przez elektroniczne zewnętrzne nośniki informacji należy rozumieć dyskietki, płyty CD i DVD, zewnętrzne dyski twarde, pendrivy, taśmy itp.
3. Na elektronicznych zewnętrznych nośnikach informacji zapis danych osobowych, w tym w szczególności zbiorów danych osobowych, może nastąpić tylko w uzasadnionych przypadkach, kiedy jest to wymagane charakterem pracy, przepisami prawa, a okres przechowywania danych osobowych na takich nośnikach powinien być ograniczony do

minimum za wyjątkiem kopii zapasowych.

4. Elektroniczne zewnętrzne nośniki informacji zawierające dane osobowe po zakończeniu pracy przechowuje się w miejscach bezpiecznych – przechowywania danych osobowych.

5. Wynoszenie poza Komendę Straży Miejskiej elektronicznych nośników informacji zawierających zbiory danych osobowych jest dopuszczalne tylko w wyjątkowych sytuacjach, kiedy jest to podyktowane przepisem prawa lub jest na to pisemna zgoda Komendanta Straży Miejskiej.

6. Osoba wynosząca elektroniczne nośniki informacji zawierające zbiory danych osobowych, jak i pojedyncze dane osobowe jest osobiście odpowiedzialna za zabezpieczenie nośników przed zniszczeniem, modyfikacją i kradzieżą.

7. Sposób usuwania danych osobowych z elektronicznych nośników informacji zawierających dane osobowe powinien być bezpieczny, uniemożliwiający odtworzenie.

8. Nieprzydatne elektroniczne nośniki informacji przekazuje się do Referatu Informatycznego celem zniszczenia.

9. Nośniki informacji: płyty CD, DVD, dyskietki, taśmy, pendrivy niszczy się na bieżąco.

10. Przed składowaniem komputerów przekazanych do likwidacji wyjmuje się dyski twarde, które przechowuje się w pokoju.

11. Okresowo niszczy się pozostałe nośniki informacji: dyski twarde w sposób uniemożliwiający odtworzenie.

Kopie zapasowe.

1. Zarządza się archiwizację danych i systemów:

- codziennie (w dni robocze) – dane w systemach wielodostępowych.
- okresowo – dla systemów autonomicznych, eksploatowanych w komórkach organizacyjnych Komendy Straży Miejskiej w Cieszynie. Za przeprowadzenie oraz określenie częstotliwości archiwizowanych danych w systemach autonomicznych odpowiedzialny jest kierownik komórki.
- w uzasadnionych przypadkach, kiedy jest to podyktowane szczególnymi przepisami, wymaganiami określonego systemu lub wewnętrznymi regulacjami, można stosować archiwizację danych i systemów w innych odstępach czasowych, jeśli nie wpływa to negatywnie na bezpieczeństwo danych i możliwość prawidłowego odtworzenia danych w sytuacjach awaryjnych.

2 Kopie archiwizacyjne za wyjątkiem systemów autonomicznych wykonują administratorzy systemu informatycznego.

3. Kopie są wykonywane całościowo.

4. Administrator systemu informatycznego dba o jakość wykonywanych kopii oraz o

możliwość ich odtworzenia w przypadku awarii.

5. Raz na pół roku sprawdza się możliwość odtworzenia pełnej kopii. Raz na dwa tygodnie sprawdza się możliwość odtworzenia kilku plików lub folderów. Codziennie sprawdza się logi z wykonania kopii.

6. Kopie archiwizacyjne należy sporządzić na dostępnych, zewnętrznych nośnikach informacji z opisem zawierającym: nazwa straży, informację o zawartości, nr kopii.

7. Bieżące kopie archiwizacyjne przechowuje się w szafie pancernej.

8. Dane z każdego z serwera są archiwizowane na dwóch kompletach taśm w cyklu tygodniowym. Raz w tygodniu w poniedziałek lub następny roboczy dzień komplet kopii przewozi się do drugiego budynku – ul. Kochanowskiego 14 - kancelaria tajna w celu zamiany taśm.

9. Przewożenie kopii mogą dokonywać wyłącznie administratorzy systemu informatycznego wraz z kierowcą.

10. Kopie przenoszone zabezpiecza się przed wpływem czynników atmosferycznych, kradzieży itp.

11. Kopie przewozi się możliwie najkrótszą drogą .

VI Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego i utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

1. Serwery i aktywne urządzenia sieciowe, służące do przetwarzania danych osobowych, zabezpiecza się przed utratą tych danych z powodu awarii zasilania lub zakłóceń w sieci zasilającej poprzez zastosowanie UPS.

2. Sprzęt komputerowy i urządzenia peryferyjne podłącza się do wyznaczonej sieci elektrycznej.

3. Zabronione jest podłączanie innych urządzeń w tym w szczególności czajników, grzejników elektrycznych, wentylatorów itp. do gniazd wydzielonej sieci elektrycznej zasilającej sprzęt komputerowy.

4. Okresowo wykonywane są przeglądy sieci elektrycznej i alarmowej i wszelkich urządzeń mających wpływ na bezpieczeństwo straży.

5. Każdy zewnętrzny elektroniczny nośnik informacji, z którego informacja wprowadzana będzie do komputera służbowego, musi uprzednio zostać sprawdzony programem antywirusowym.

6. System sam automatycznie aktualizuje program antywirusowy w przypadku braku

aktualizacji należy powiadomić administratorów systemu informatycznego.

VII Informacja o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

1. Użytkownik zobowiązany jest prowadzić wykaz udostępnień danych w aplikacji przetwarzającej dane osobowe, a dla aplikacji, które nie umożliwiają odnotowania takich danych w oddzielnym
wykazie. Wykaz powinien zawierać nazwę odbiorcy, datę i zakres udostępnienia.
2. Zgodnie z ustawą o ochronie danych osobowych przez odbiorcę danych należy rozumieć każdego, komu udostępnia się dane, z wyłączeniem: osoby, której dane dotyczą; osoby upoważnionej do przetwarzania danych; przedstawiciela podmiotu w Rzeczypospolitej Polskiej, który ma siedzibę lub miejsce zamieszkania w państwie trzecim; podmiotu, któremu powierzyło się przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

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

1. Wykonywania przeglądów i konserwacji systemów oraz nośników informacji przeprowadza się zgodnie z instrukcją dla danego urządzenia, w pozostałych przypadkach zgodnie z procedurą ustaloną przez Kierownika Referatu Informatycznego.
2.W przypadku kiedy konserwacji i przeglądów dokonują firmy zewnętrzne nadzór nad tymi pracami wykonują administratorzy systemu informatycznego.
3. Należy dołożyć szczególnej staranności, aby podczas wykonywania takich czynności nie doszło do utraty danych, modyfikacji danych lub wglądu do danych przez osobę nieupoważnioną.
4. W przypadku kiedy nie ma możliwości wykonania czynności naprawczych, konserwacyjnych
w Komendzie, urządzenia przed przekazaniem pozbawia się wszelkich nośników zawierających dane osobowe.

IX. Bezpieczeństwo komputerów przenośnych.

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialny jest Komendant, w którego posiadaniu jest komputer lub inne osoby, które zostały bezpośrednio wyznaczone do użytkowania danego komputera przenośnego.
2. Użytkownicy, którym zostały powierzone komputery przenośne, zobowiązani są 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 identyfikatora użytkownika.

5. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni.

6. Przetwarzanie danych osobowych w komputerach przenośnych dopuszczalne jest tylko w uzasadnionych przypadkach, kiedy jest to podyktowane charakterem pracy i są spełnione wszystkie wymogi bezpieczeństwa dla komputerów przenośnych służących do przetwarzania danych osobowych.

7. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub wypisów za wyjątkiem sytuacji, kiedy istnieje umotywowana potrzeba przetwarzania takich danych, a użytkownik posiada pisemną zgodę Komendanta Straży Miejskiej oraz dane zostały zabezpieczone kryptograficznie.

8. Zabrania się pracy na komputerach przenośnych, w miejscach ogólnie dostępnych, gdzie może dojść do podglądnięcia danych osobowych przez osoby do tego nieupoważnione.

9. Zabrania się pozostawiania komputera przenośnego bez nadzoru osoby upoważnionej w miejscach, gdzie istnieje możliwość łatwego pozyskania danych lub kradzieży komputera,

np. w recepcji, w szatni, w samochodzie.

10. W komputerze przenośnym przechowuje się tylko taki zakres danych, który jest niezbędny do wykonywania bieżącej pracy. W pozostałych przypadkach usuwa się te dane lub archiwizuje.

11. Za archiwizację danych w komputerach przenośnych odpowiadają użytkownicy, którzy przetwarzają te dane.

KOMENDANT
STRAŻY MIEJSKIEJ
W CIESZYNIE
mgr Kazimierz Ptusa