tylko za pisemną zgodą Komendanta Straży Miejskiej.

f/ W pomieszczeniach, gdzie przetwarza się dane osobowe wprowadza się zakaz nagrywania filmów, wykonywania zdjęć oraz nagrań audio bez wcześniejszej zgody Komendanta Straży Miejskiej, w tym m. in. wykorzystywania telefonów komórkowych do w/w funkcji.

21. Obowiązki pracownika rozpoczynającego i kończącego pracę:

a/ Rozpoczynając pracę pracownik powinien pobrać klucze od strażnika - dyżurnego (pomocnika). Dyżurny (pomocnik) powinien mieć szczególny nadzór nad kluczami pomieszczeń Komendy pobieranymi lub zdawanymi przez pracowników. Tylko on ma prawo wydawania i odbioru kluczy. Naganne jest zostawianie kluczy w drzwiach, bezpośrednie przekazywanie kluczy osobom wykonującym pracę w Komendzie w godzinach popołudniowych bez pośrednictwa dyżurnego (pomocnika), pozostawianie lub pobieranie kluczy w „dyżurce" bez wiedzy dyżurnego (pomocnika), zostawianie kluczy w miejscach łatwo dostępnych dla osób nieuprawnionych.

b/ W przypadku zauważenia naruszenia zabezpieczeń, zastania otwartych drzwi, uszkodzeń elementów zabezpieczających pracownik powinien zgłosić to bezpośrednio przełożonemu, który o tym fakcie powiadamia Komendanta Straży Miejskiej.

c/ Pomieszczenia służbowe winny być zamknięte każdorazowo pod nieobecność osób w nich pracujących.

d/ Osoby postronne mogą przebywać w pomieszczeniach Komendy tylko w obecności pracowników lub upoważnionych osób, a w pomieszczeniach gdzie przetwarzane są dane osobowe w obecności pracowników upoważnionych do przetwarzania danych osobowych.

e/ Kończąc pracę pracownik powinien wyłączyć zgodnie z przepisami wszystkie urządzenia, które nie wymagają ciągłego zasilania. Uporządkować swoje stanowisko pracy, a w szczególności zamknąć pieczątki, zniszczyć w sposób uniemożliwiający odzyskanie wszystkie tymczasowe wydruki komputerowe zawierające dane osobowe, a w przypadku kiedy będą jeszcze użytkowane zamknąć je w miejscach przechowywania danych osobowych. Przez miejsca przechowywania danych osobowych należy rozumieć szafy drewniane, metalowe itp. z możliwością zamknięcia na zamek, gdzie nie ma możliwości dostępu osób nieupoważnionych. Szczegółowe miejsca przechowywania danych osobowych wyznacza Komendant Straży Miejskiej. Elektroniczne zewnętrzne nośniki

informacji (dyskietki, płyty CD itp.) zawierające dane osobowe zamyka się również w/w miejscach przechowywania danych osobowych.

f/ Zabrania się wynoszenia poza teren Komendy wydruków komputerowych, ksiąg, kartotek, akt oraz innych nośników zawierających zbiory danych osobowych w tym dyskietek, CD-romów, dysków i innych elektronicznych nośników danych oraz komputerów o ile nie jest to podyktowane przepisem prawa lub nie ma na to pisemnej zgody Komendanta Straży Miejskiej.

g/ W przypadku kiedy jest konieczne wyniesienie nośników z danymi osobowymi poza teren Komendy osoba bezpośrednio odpowiedzialna za dane powinna dołożyć szczególnej staranności, aby nie doszło do utraty danych w tym kradzieży, zniszczenia, modyfikacji. Dane powinny być zabezpieczone przed wpływami czynników atmosferycznych oraz dostępem do nich osób nieuprawnionych. Transport powinien się odbywać drogą możliwie najkrótszą do miejsca docelowego.

h/ Przesyłanie zbiorów danych osobowych pocztą elektroniczną lub poprzez protokół ftp na serwer firm, instytucji zewnętrznych może następować tylko i wyłącznie w uzasadnionych przypadkach za pisemną zgodą Komendanta Straży Miejskiej lub kiedy wynika to z przepisów prawa.

i/ Przesyłane zbiory muszą być zabezpieczone w sposób uniemożliwiający odczyt przez osobę nieuprawnioną.

j/ Za bezpieczeństwo przenoszonych lub udostępnianych danych w tym zbiorów danych osobowych odpowiedzialna jest bezpośrednio osoba udostępniająca i przenosząca dane.

k/ Opuszczając pomieszczenie wszystkie szafy zawierające dane osobowe oraz okna i drzwi wejściowe do biura powinny być zamknięte na wszystkie istniejące zamki. W przypadku nie działania, któregokolwiek z zabezpieczeń powinno to być jak najszybciej zgłoszone Komendantowi Straży Miejskiej.

22.Zabezpieczenie komputera i praca na komputerze:

a/ W pomieszczeniach, w których odbywa się przetwarzanie danych osobowych, a jednocześnie mają do tych pomieszczeń dostęp osoby postronne, monitory urządzeń komputerowych muszą być ustawione w taki sposób, by informacje na nich wyświetlane nie były widoczne dla osób postronnych.

b/ Dostęp do systemu oraz oprogramowania służącego do przetwarzania danych osobowych powinien być poprzedzony wprowadzeniem identyfikatora i hasła.

c/ Zabronione jest udostępnianie innym osobom hasła i identyfikatora. Każdy

użytkownik odpowiada za swój identyfikator i hasło oraz za wykonane z ich pomocą operacje w systemach komputerowych.

d/ Hasło musi być zmieniane nie rzadziej niż co 30 dni, zawierać co najmniej 8 znaków, składać się z małych i wielkich liter oraz cyfr lub znaków specjalnych.

e/ Zabrania się przechowywania haseł w systemach komputerowych w niechronionej postaci oraz zapisywania ich na karteczkach, kalendarzach itp.

f/ Zabrania się używania tych samych haseł w systemach służbowych i prywatnych.

g/ Dla urządzeń komputerowych mających odpowiednie możliwości techniczne, ekrany monitorów muszą być automatycznie wygaszane w przypadku ponad 15 minutowej nieaktywności użytkownika.

h/ Każda osoba opuszczająca na dłużej stanowisko pracy powinna wylogować się z aplikacji i z systemu.

i/ Dyskietki, CD i inne zewnętrzne nośniki danych mogą być odczytywane na komputerach służbowych, tylko i wyłącznie po wcześniejszym sprawdzeniu programem antywirusowym.

j/ Każdy użytkownik komputera zobowiązany jest do używania w pracy tylko dyskietek, płyt CD, DVD i innych zewnętrznych nośników informacji zakupionych przez Komendę (nie prywatnych) lub przekazanych przez inne instytucje w celu wykonania określonych prac. Należy przechowywać na nich tylko i wyłącznie dane związane z charakterem pracy. Zewnętrzne nośniki informacji powinny być oznaczone zgodnie z instrukcją kancelaryjną.

k./ Należy pamiętać, że na dyskietkach pendrivach itp. dane są możliwe do odczytania pomimo ich usunięcia.

l/ Na wszystkich komputerach Komendy Straży Miejskiej dopuszcza się instalację tylko legalnego i licencjonowanego oprogramowania zainstalowanego przez informatyków Komendy.

ł/ System informatyczny zabezpiecza się w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

m/ Zabrania się pobierania z internetu oprogramowania oraz innych plików nie związanych z charakterem pracy.

n/ Korzystanie z internetu oraz z poczty elektronicznej jest dozwolone tylko w celach służbowych.

o/ Zabrania się zapisywania danych osobowych i innych ważnych danych na dyskach lokalnych, jeśli nie jest to wymuszone względami technicznymi.

p/ Zabrania się przechowywania na dyskach lokalnych, dyskach sieciowych i zewnętrznych nośnikach informacji danych nie związanych z charakterem pracy, w tym np.: filmów, muzyki, zdjęć, programów itp.

r/ Zabrania się samowolnego poprawiania zapisów komputerowych dotyczących danych rejestracyjnych, ingerencji w aplikacje itp. mogących spowodować nieprawidłową ich pracę lub utratę danych.

s/ Wszyscy pracownicy, użytkownicy, jak również strony trzecie, mające dostęp do systemów informatycznych i pomieszczeń są zobowiązani do odnotowywania i raportowania wszystkich słabych punktów systemu bezpieczeństwa i zgłaszania tego przełożonym lub nadzorującym ich pracę.

23. Szczegółowe postępowanie z systemem informatycznym określa Instrukcja zarządzania systemem informatycznym.

24. Dla określonych systemów, aplikacji, zbiorów jak również budynków i pomieszczeń mogą być wprowadzane szczegółowe polityki bezpieczeństwa, instrukcje zarządzania systemem informatycznym oraz regulaminy postępowania jeżeli będą miały wpływ na zwiększenie bezpieczeństwa przetwarzanych danych.

25. W przypadku kiedy dane zbiory, programy lub szczegółowe przepisy lub uregulowania wymagają dalej idącej ochrony należy je stosować.

26. Wymagania dotyczące zawierania zapisów z zakresu bezpieczeństwa danych w zawieranych umowach.

a/ W przypadku, kiedy realizacja umowy z osobami trzecimi będzie wymagać dostępu do pomieszczeń, urządzeń, gdzie przetwarzane są dane osobowe lub istnieje prawdopodobieństwo dostępu do takich pomieszczeń należy dołożyć szczególnej staranności, aby umowa bazowała na formalnych zapisach dotyczących bezpieczeństwa lub odnosiła się do odpowiednich dokumentów bezpieczeństwa i regulacji prawnych w tym ustawy o ochronie danych osobowych.

b/ W przypadku przetwarzania danych zapisy dotyczące bezpieczeństwa danych, mogą stanowić część umowy zasadniczej dotyczącej określonego przedmiotu umowy lub stanowić odrębną umowę dotyczącą powierzenia przetwarzania danych osobowych w zakresie niezbędnym do wykonania określonych czynności.

c/ Osoba nadzorująca pracę firm lub innych osób w komendzie jest zobowiązana poinformować o zasadach polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w urzędzie, które mają szczególny wpływ na

bezpieczeństwo danych podczas prowadzonych przez nich prac.

d/ Samo powierzenie przetwarzania danych może nastąpić tylko w uzasadnionych przypadkach, kiedy jest to zgodne z przepisami prawa.

e/ Za wprowadzenie do umów w/w zapisów odpowiada osoba bezpośrednio przygotowująca umowę oraz Komendant, który odpowiedzialny jest za dany zbiór lub bezpośrednie bezpieczeństwo w danym pomieszczeniu.

f/ Każda umowa musi zostać zaparafowana przez Radcę Prawnego Komendy Straży Miejskiej w Cieszynie.

g/ Kopia umowy powierzenia przetwarzania danych osobowych musi zostać dostarczona do Administratora Danych.

VI. POSTĘPOWANIE W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Naruszenie systemu ochrony danych osobowych może być stwierdzone na podstawie: stanu urządzeń zabezpieczających, zawartości zbiorów danych osobowych, sposobu działania oprogramowania i sieci informatycznej itp.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy:

a/ zabezpieczyć pomieszczenie, zablokować dostęp do systemu informatycznego dla użytkowników oraz osób nieupoważnionych,

b/ powiadomić Komendanta Straży Miejskiej, który powiadamia o zaistniałej sytuacji Burmistrza Miasta,

c/ wyznaczona przez Komendanta Straży Miejskiej osoba podejmuje działania wyjaśniające mające na celu ustalenie przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych, osób winnych naruszenia bezpieczeństwa danych oraz skutków naruszenia.

d/ wyznaczona przez Komendanta Straży Miejskiej osoba przygotowuje pisemny raport dotyczący zaistniałej sytuacji i przekazuje go Komendantowi Straży Miejskiej, który podejmuje dalsze działania.

3. Odpowiedzialność:

a/ Za nieprzestrzeganie zapisów Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym wobec pracownika mogą zostać wyciągnięte konsekwencje zgodnie z Kodeksem pracy.

b/ Wobec osób trzecich i firm na zasadzie odrębnych przepisów.

KOMENDANT
STRAŻY MIEJSKIEJ
W CIESZYNIE
mgr Kazimierz Pusa