INSTRUKCJA ZARZĄDZANIA SYSTEMEM MONITORINGU WIZYJNEGO PŁYWALNI MIEJSKIEJ W KOLE

I. POSTANOWIENIA OGÓLNE

Instrukcja zarządzania systemem monitoringu wizyjnego służącym do przetwarzania danych osobowych zwana dalej "Instrukcją" została opracowana zgodnie z wymogami § 5 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. Z 2004 r. Nr 100, poz. 1024).

II. DOKUMENTY POWIĄZANE

1. Polityka bezpieczeństwa przetwarzania danych osobowych w systemie monitoringu wizyjnego Pływalni Miejskiej w Kole
2. Projekt systemu monitoringu wizyjnego Pływalni Miejskiej w Kole.

III. DEFINICJE

1. **Administrator danych** – Burmistrz Miasta Koła.
2. **Administrator Bezpieczeństwa Informacji** – wyznaczona osoba, odpowiedzialna w szczególności za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w systemach informatycznych oraz zbiorach nieinformatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
3. **Administrator systemu monitoringu wizyjnego** – osoba, która otrzymuje zlecenie konserwacji czy naprawy sprzętu w przypadku takiej konieczności. Dostęp do systemu i infrastruktury monitoringu miejskiego wymaga każdorazowej pisemnej zgody Kierownika Wydziału ds. obsługi krytej pływalni.

4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołania się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
5. **Osoba upoważniona** – osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę wyznaczoną (Administratora Bezpieczeństwa Informacji), uprawniona do przetwarzania danych osobowych.
6. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
7. **Rozporządzenie** – 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. z 2004 r. Nr 100, poz. 1024).
8. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
9. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie monitoringu wizyjnego.
10. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
11. **Pomieszczenie monitoringu wizyjnego** – mamy na myśli pomieszczenia zlokalizowane w budynku Pływalni Miejskiej w Kole.
12. **Monitoring wizyjny** – mamy na myśli ogół pomieszczeń Krytej Pływalni w Kole i pracowników zatrudnionych w Wydziale ds. obsługi krytej pływalni oraz zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
13. **Zbiór o nazwie „Monitoring wizyjny Pływalni Miejskiej w Kole"** - mamy na myśli zbiór danych osobowych zarejestrowany w GIODO, do którego dostęp mają pracownicy Wydziału ds. obsługi krytej pływalni w Kole, posiadający wydane przez Administratora Bezpieczeństwa Informacji upoważnienia do dostępu do danych zawartych w zbiorze.

14. **Kierownik** – mamy na myśli Kierownika Wydziału ds. obsługi krytej pływalni.
15. **Z–ca Kierownika** – mamy na myśli z–ce Kierownika Wydziału ds. obsługi krytej pływalni.
16. **Projekt systemu monitoringu wizyjnego** – dokument zawierający rozmieszczenie poszczególnych kamer oraz podstawowe informacje o ich parametrach, wykaz pomieszczeń lub ich części, w których przetwarzane są dane zarejestrowane przez kamery systemu, wykaz zbiorów zawierających dane zebrane w systemie, wykaz powiązań między nimi oraz wykaz programów i procedur służących do przetwarzania danych.

IV. ZAKRES I CEL INSTRUKCJI

1. Celem Instrukcji jest określenie podstawowych zasad właściwego zarządzania systemem monitoringu wizyjnego, służącym do przetwarzania danych osobowych oraz podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład, urządzenia, odpowiednio do zagrożeń i kategorii danych objętych ochroną.
2. Instrukcję stosuje się do danych osobowych przetwarzanych w systemach monitoringu wizyjnego, danych osobowych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji o sposobach zabezpieczenia danych osobowych.
3. Przy przetwarzaniu danych osobowych w systemach monitoringu wizyjnego należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia, ponieważ urządzenia systemu służącego do przetwarzania danych osobowych połączone są z siecią publiczną.
4. Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem monitoringu wizyjnego. W przypadku, gdy z oceny funkcjonowania instrukcji wynika, że zachodzi potrzeba wprowadzenia nowych lub modyfikacji istniejących zasad właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, wnioski w tej sprawie powinni składać operatorzy systemu do Administratora Bezpieczeństwa Informacji za pośrednictwem Kierownika.

V. ZABEZPIECZENIE DANYCH OSOBOWYCH W SYSTEMIE MONITORINGU WIZYJNEGO

1. Zapewnienie bezpieczeństwa danych osobowych powinno być jednym z najistotniejszych czynników przy wyborze oprogramowania wchodzącego w skład systemu monitoringu wizyjnego, który ma służyć do przetwarzania danych osobowych.
2. Wdrożenie zabezpieczeń systemów monitoringu wizyjnego służących do przetwarzania danych osobowych, ma służyć zapewnieniu jak najwyższego poziomu bezpieczeństwa tych danych, które są w nich przetwarzane, przy uwzględnieniu jednak ograniczonych możliwości finansowych Administratora danych oraz istniejących już rozwiązań technicznych i organizacyjnych w tym zakresie.
3. W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu monitoringu wizyjnego przetwarzającego dane osobowe powinien być możliwy wyłącznie po uwierzytelnieniu użytkownika zgodnie z zasadami określonymi w Polityce.
4. Prawidłowy poziom zabezpieczenia systemu monitoringu wizyjnego służącego do przetwarzania danych osobowych zostaje zapewniony poprzez przestrzeganie następujących zasad:
   1) uniemożliwienie osobom postronnym uzyskiwania nieupoważnionego dostępu do systemu;
   2) instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania wyłącznie przez uprawnionych użytkowników systemu;
   3) niepodejmowanie przez użytkowników systemu prób testowania, modyfikacji i naruszenia zabezpieczeń systemu lub jakichkolwiek działań noszących takie znamiona;
5. Dostęp do infrastruktury technicznej związanej z siecią teleinformatyczną oraz jej zasilaniem powinien być wyłącznie dla osób uprawnionych i zatwierdzonych w sposób formalny.
6. Urządzenia logiczne sieci, rozdzielnie elektryczne, centrale telefoniczne oraz skrzynki z bezpiecznikami powinny posiadać skuteczną ochronę przed dostępem osób nieuprawnionych.
7. Pomieszczenie monitoringu wizyjnego zabezpiecza się przed dostępem osób nieuprawnionych za pomocą drzwi drewnianych z jednym zamkiem patentowym.
8. Przebywanie osób postronnych w pomieszczeniach służbowych monitoringu jest niedopuszczalne. Wyjątek stanowią funkcjonariusze Policji, Żandarmerii Wojskowej

i innych służb mundurowych na pisemne polecenia dowódcy danej jednostki, tylko i wyłącznie w celach dochodzeniowych, śledczych, dowodowych, po wcześniejszym wylegitymowaniu.

9. Osobami upoważnionymi do wprowadzenia w obszar monitoringu innych osób postronnych są: Burmistrz Miasta Koła, Kierownik i jego zastępca.

VI. OBOWIĄZKI UŻYTKOWNIKÓW SYSTEMU

1. Do podstawowych obowiązków użytkowników systemu monitoringu wizyjnego należy przetwarzanie danych osobowych wyłącznie w celu i zakresie wynikającym z obowiązków służbowych.
2. Użytkownicy systemu monitoringu wizyjnego zobowiązani są do podejmowania współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu. Wszelkie zauważone nieprawidłowości zobowiązani są zgłaszać do Kierownika lub Administratora Bezpieczeństwa Informacji.
3. Użytkownicy systemu monitoringu wizyjnego zobowiązani są do:
   1) przestrzegania opracowanych dla systemu zasad przetwarzania danych osobowych oraz procedur i instrukcji;
   2) uniemożliwienia dostępu lub podglądu danych osobom nieupoważnionym;
   3) informowania Kierownika lub Administratora Bezpieczeństwa Informacji o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;
   4) wykonywania bez zbędnej zwłoki poleceń Administratora danych lub Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

VII. NADAWANIE, ZMIAN LUB USUWANIE UPRAWNIEŃ DO SYSTEMU MONITORINGU WIZYJNEGO

1. Upoważnienia do przetwarzania danych osobowych w ramach monitoringu wizyjnego nadawane są zgodnie z zakresem czynności służbowych na wniosek Kierownika przez Administratora Bezpieczeństwa Informacji.
2. Zmiany dotyczące użytkownika systemu monitoringu wizyjnego, takie jak rozwiązanie umowy o pracę lub zmiana zakresu czynności służbowych są przesłanką

do unieważnienia upoważnienia o którym mowa w pkt. 1 i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych.

3. Prawa dostępu przyznane użytkownikom systemu, którzy nie są pracownikami etatowymi Administratora danych powinny mieć charakter czasowy i mogą być przyznawane wyłącznie na okres odpowiadający wykonywanemu zadaniu oraz powinny być formalnie zatwierdzane.

VIII. METODY I ŚRODKI UWIERZYTELNIANIA W SYSTEMIE MONITORINGU WIZYJNEGO

1. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom systemu monitoringu wizyjnego rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższej zasady: użytkownik systemu realizuje swoje zadania służbowe związane z obsługa monitoringu wizyjnego wyłącznie w czasie pracy, który ustalony został w grafiku pracy. Obecność na stanowisku pracy odnotowywana jest na liście obecności.

IX. HASŁA W SYSTEMIE REJESTRATORÓW NAGRAŃ

1. Loginem i hasłem zabezpieczone są rejestratory nagrań z monitoringu wizyjnego. Dostęp do rejestratorów nagrań posiada Kierownik, zastępca Kierownika oraz upoważniony pracownik. Hasła powinny być tj.:
   1) długości co najmniej 8 znaków,
   2) które są łatwe do zapamiętania, a trudne do odgadnięcia,
   3) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.),
   4) w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra, znak specjalny.
2. Hasło dostępu do rejestratorów jest zmieniane w przypadku takiej konieczności. O zmianie hasła decyduje Kierownik.
3. Należy unikać ponownego lub cyklicznego używania haseł, które już kiedyś były wykorzystywane.

4. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
5. Hasła nie powinny być przechowywane oraz przesyłane w postaci jawnej.

X. ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY W SYSTEMIE

1. Przed przystąpieniem do pracy z systemem monitoringu wizyjnego, użytkownik systemu zobowiązany jest dokonać sprawdzenia stanu urządzeń monitoringu miejskiego oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie Kierownika lub Administratora danych albo Administratora Bezpieczeństwa Informacji.
3. W przypadku konieczności opuszczenia stanowiska przez operatora pomieszczenie monitoringu jest zamykane na klucz.

XI. REJESTRACJA NAGRAŃ ZAPISÓW MONITORINGU MIEJSKIEGO

1. Dane osobowe przetwarzane w systemie monitoringu wizyjnego zapisywane są na rejestratorach wizji SDVR916P-600, do których dostęp posiadają upoważnione osoby.
2. Stanowisko nadzoru wizyjnego zlokalizowane jest na parterze w pomieszczeniu ochrony w obiekcie Pływalni Miejskiej w Kole.
3. Rejestrator, do którego spływają dane z kamer obiektowych znajduje się również w pomieszczeniu ochrony w obiekcie Pływalni Miejskiej w Kole.

XII. PRZECHOWYWANIE NOŚNIKÓW ELEKTRONICZNYCH ZAWIERAJĄCYCH DANE OSOBOWY

1. Dane osobowe mogą być przechowywane:
   a) na serwerach
   b) na stacjach roboczych.
2. Nośniki elektroniczne zawierające dane osobowe, dla których cel przetwarzania ustał powinny być pozbawiane zapisu tych danych a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie / odzyskanie danych osobowych.

XIII. OCHRONA SYSTEMU PRZED DZIAŁANIEM SZKODLIWEGO OPROGRAMOWANIA

1. System monitoringu wizyjnego służący do przetwarzania danych osobowych zabezpieczony jest przed nieuprawnionym dostępem do systemu monitoringu wizyjnego poprzez zastosowane oprogramowanie antywirusowe.
2. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
3. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik systemu nie był w stanie wyłączyć lub pominąć etapu skanowania.
4. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instaluje Administrator systemu monitoringu wizyjnego niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
5. Wyznaczone osoby mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

XIV. FUNKCJONALNOŚĆ SYSTEMU MONITORINGU WIZYJNEGO

1. W systemie monitoringu wizyjnego do celów archiwizacyjnych, rejestracyjnych i podglądowych zbiorów, stosuje się system Player V2.12.0
2. System nagrywa obraz bez dźwięku w czasie rzeczywistym. Przeglądanie materiału możliwe jest przez podanie określonej daty i godziny.
3. Do zbioru Monitoring wizyjny dostęp mają wyłącznie osoby, którym wydane zostało stosowne upoważnienie do przetwarzania danych osobowych w tym zbiorze.
4. Dostęp do zbioru danych osobowych – monitoring wizyjny, w celach serwisowych, posiadają pracownicy firmy serwisowej na podstawie trwającej gwarancji wykonawcy. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.
5. Poza bieżącą rejestracją na dyskach, pracownicy pływalni prowadzą bieżący rejestr zdarzeń, wymagających interwencji służb tj.: Policja, Straż Miejska, Pogotowie Ratunkowe, Straż Pożarna, inne służby miejskie.

6. Wpisy we wspomnianym rejestrze dokonywane są w sposób chronologiczny. Umożliwia to szybką identyfikację określonego zbioru danych.
7. System monitoring wizyjnego nie stosuje dodatkowej zaawansowanej analizy obrazu.

XV. ZASADY MONITOROWANIA, PRZEGLĄDU O KONSERWACJI SYSTEMU

1. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiada Kierownik Wydziału ds. obsługi krytej pływalni.
2. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności Kierownika lub innej wyznaczonej przez niego osoby.
3. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu monitoringu wizyjnego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia. o której mowa w art. 31 ustawy o ochronie danych osobowych.
4. Osoby nie będące pracownikami, które prowadzą prace serwisowe na rzecz Administratora danych przed rozpoczęciem prac, powinny być poddane weryfikacji tożsamości przez Kierownika bądź jego Z-cę lub inną wyznaczoną do tego celu osobę.
5. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.

XVI. PRZETWARZANIE DANYCH POZA OBSZAREM PRZETWARZANIA

1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe w tym dane wrażliwe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych.
2. Umożliwia się przekazywanie i wgląd do zbiorów danych osobowych upoważnionym do tego służbom (Policja, Prokuratura, Sąd) na podstawie pisemnego wniosku kierownika danej jednostki.

3. Dane przekazywane są na nośnikach zewnętrznych w postaci płyty CD lub DVD wyłącznie upoważnionym do tego służbom (Policja, Straż Miejska, Prokuratura, Sąd) .
4. Przekazanie danych odbywa się tylko i wyłącznie poprzez osoby do tego uprawnione: Kierownik Wydziału ds. obsługi krytej pływalni oraz jego zastępca.
5. Fakt przekazania danych odnotowywany jest w ewidencji w sposób chronologiczny pod symbolem OP. 5520.

XVII. POSTANOWIENIA KOŃCOWE

1. Naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy, zgodnie z Kodeksem Pracy
2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t. j. Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
3. Użytkownicy systemu zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji, w wypadku odrębnych od zawartych w niniejszej Instrukcji uregulowań występujących w innych procedurach obowiązujących u Administratora danych, użytkownicy systemu mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych przetwarzanych w systemie informatycznym.

BURMISTRZ
Mieczysław Drożdżewski

ADMINISTRATOR
Bezpieczeństwa Informacji
Andrzej Bednarkiewicz