

Zarządzenie Nr 57.2013
Wójta Gminy Przytyk
z dnia 15 listopad 2013 r.

**w sprawie: wdrożenia dokumentacji przetwarzania i ochrony danych osobowych
z systemu monitoringu wizyjnego w Przytyku**

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (jt. Dz. U. z 2013 r. Nr 594 z późn. zm.), w związku z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 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

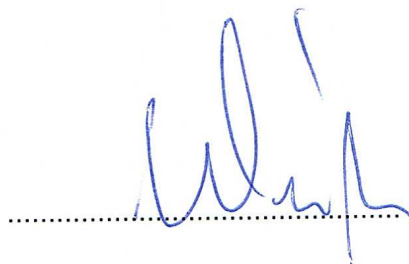
1. Wprowadzam do stosowania:
„Politykę bezpieczeństwa przetwarzania danych osobowych z systemu monitoringu wizyjnego w Przytyku” - w brzmieniu stanowiącym załącznik nr 1 do Zarządzenia.
2. Wprowadzam do stosowania:
„Projekt systemu monitoringu wizyjnego w Przytyku” - w brzmieniu stanowiącym załącznik nr 2 do Zarządzenia.

§ 2

1. Wykonanie zarządzenia powierzam Sekretarzowi Urzędu Gminy Przytyk.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.



POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH Z SYSTEMU MONITORINGU W PRZYTyku

I. Postanowienia ogólne.

Polityka bezpieczeństwa przetwarzania danych osobowych zwana dalej „Polityką”, została wydana w związku z § 3 ust. 1 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 system monitoringu służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

II. Dokumenty powiązane.

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Przytyk
2. Projekt systemu monitoringu w Przytyku

III. Definicje.

1. Administrator danych – Gmina Przytyk, która decyduje o środkach i celach przetwarzania danych osobowych reprezentowana przez Wójta wykonującego swoje zadania przy pomocy Urzędu.
2. Administrator Bezpieczeństwa Informacji – wyznaczona osoba, odpowiedzialna w szczególności za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w systemie monitoringu 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 – wyznaczona osoba odpowiedzialna za funkcjonowanie infrastruktury systemu monitoringu, na którą składa się cały sprzęt i oprogramowanie systemu monitoringu, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemie monitoringu.
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, 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 system monitoringu miejskiego 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 (operator/współpracownik) – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie monitoringu.
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 w Przytyku – mamy na myśli pokoje nr 26 w budynku Urzędu Gminy w Przytyku przy ul. Zachęta gdzie znajduje rejestrator lub/i monitor, na którym odtwarzany jest obraz z kamer
12. System monitoringu wizyjnego – termin używany wymiennie z system CCTV, system dozoru CCTV za Polską Normą: „System składający się z punktów kamerowych, urządzeń kontrolnych, oraz urządzeń do przesyłu i sterowania, system może być niezbędny do dozoru określonej strefy bezpieczeństwa.”
13. Projekt systemu monitoringu w Przytyku – dokument zawiązujący rozmieszczenie poszczególnych kamer oraz podstawowe informacje o ich parametrach, wykaz pomieszczeń lub ich części, w których przetwarzane są dane zarejestrowane przez kamery systemu,
14. Zdarzenie – każda sytuacja zdefiniowana przez użytkownika systemu CCTV, którą system powinien wykryć i/lub na nią zareagować, np. przestępstwo, awaria instalacji, naruszenie przestrzeni prywatnej, działanie pracownika niezgodne z procedurą, itd.
15. Przestrzeń publiczna – przestrzeń, do której użytkownicy mają nieograniczony dostęp, np. przestrzeń na terenie Przytyka lub droga publiczna.
16. Przestrzeń pół-publiczna – przestrzeń prywatna, udostępniona innym osobom na warunkach określonych przez właściciela
17. Konstytucyjna zasada proporcjonalności – w odniesieniu do systemów monitoringu wizyjnego, jest to taki zakres prowadzonej obserwacji, rejestracji obrazu, przechowywania nagrań i przetwarzania danych z systemu CCTV, który umożliwia realizację celów przez właściciela lub zarządzającego obszarem objętym nadzorem i w jak najmniejszy sposób narusza prawa i wolności osób, które znajdują się na tym obszarze.

IV. Zakres oraz cel Polityki.

1. Celem polityki jest określenie podstawowych zasad właściwego zarządzania systemem monitoringu, oraz podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład, urządzenia, odpowiednio do zagrożeń i kategorii danych objętych ochroną.
2. Politykę stosuje się do danych osobowych przetwarzanych w systemie monitoringu, danych osobowych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji o sposobach zabezpieczenia danych osobowych, o których mowa w art. 39 ust. 3 ustawy.
3. Przy przetwarzaniu danych osobowych w systemach monitoringu 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. Polityka zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem monitoringu. W przypadku, gdy z oceny funkcjonowania instrukcji wynika, że zachodzi potrzeba wprowadzenia nowych lub modyfikacji istniejących zasad właściwego zarządzania systemem monitoringu służącym do przetwarzania danych osobowych, wnioski w tej sprawie powinni składać użytkownicy systemu do Administratora Systemu Monitoringu.

V. Zarządzanie ochroną danych osobowych.

1. Obserwacja i zapis obrazu na elektronicznych nośnikach informacji - oprócz doraźnego celu, jakim jest obserwacja, istnieją inne cele np. zapamiętanie obrazu dla celów dowodowych, lub zapewnienie możliwości ponownej jego obserwacji w celu przyjrzenia się jego szczegółom.
2. Zapisywanie obrazu odbywa się w celu zapewnienia możliwości jego odtworzenia w przyszłości - rejestracja obrazu służy głównie celom dowodowym i prewencyjnym tj. zniechęcającym do popełnienia zabronionych czynów na skutek łatwych możliwości ich wykrycia
3. Dane zapisywane w systemie przechowywane są nie krócej niż 14 dni.
4. Administrator danych zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
5. Zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników monitoringu.
6. Pracownicy monitoringu przed dopuszczeniem do przetwarzania danych osobowych, muszą zostać przeszkoleni w zakresie ochrony danych osobowych. Za opracowanie programu szkolenia i przeprowadzenie szkolenia odpowiada Administrator Bezpieczeństwa Informacji.
7. W imieniu Administratora danych nadzór nad przestrzeganiem zasad ochrony danych osobowych sprawuje Administrator Systemu.

VI. Upoważnienie do przetwarzania danych osobowych.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych i złożyły oświadczenie o zachowaniu w poufności danych i sposobów zabezpieczeń. .
2. Upoważnienie wraz z oświadczeniem do przetwarzania danych osobowych obowiązuje do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.
3. Upoważnienia wraz z oświadczeniem pracownika, o których mowa powyżej przechowywane są w aktach osobowych pracownika.

VII. Ewidencja osób upoważnionych do przetwarzania danych osobowych.

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną i zawiera:
 - 1) Imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych.
 - 2) Zakres upoważnienia do przetwarzania danych osobowych.
 - 3) Identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie monitoringu, służącym do przetwarzania danych osobowych.
 - 4) Datę nadania i odebrania uprawnień.
2. Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia, które uzasadniały udzielenie im dostępu do danych osobowych.

VIII. Obszary przetwarzania danych osobowych.

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych. Do takich pomieszczeń, zalicza się:
 - 1) pomieszczenie, w którym zlokalizowany jest rejestrator.
 - 2) gabinet Wójta

- 3) pomieszczenia, w których przechowuje się zbiory nieinformatyczne, dokumenty źródłowe oraz wydruki z systemu monitoringu zawierające dane osobowe;
 - 4) pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.
2. Zbiory papierowe, wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
3. Niepotrzebne wydruki lub inne dokumenty należy niszczyć w niszczarkach.

IX. Wykaz zbiorów danych osobowych.

1. Dane osobowe gromadzone we wskazanym zbiorze są przetwarzane w systemie monitoringu oraz w rejestrach nieinformatycznych, które są zlokalizowane w pomieszczeniach należących do obszaru przetwarzania danych osobowych.

X. Powierzenie przetwarzania danych osobowych.

1. Powierzenie przetwarzania danych osobowych może mieć miejsce na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać też zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.
2. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 31 i nast. Ustawy. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39a Ustawy.
3. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Administratora danych i osób przez niego upoważnionych za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Administratora danych do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki, dokumentów powiązanych i właściwych przepisów prawa.

XI. Udostępnianie danych osobowych.

1. Dane osobowe mogą być udostępniane zgodnie z art. 27 ust. 2 pkt 1-5 ustawy.
2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora danych. Zgoda, o ile nie zmieni się cel wykorzystania danych oraz podmiot, któremu dane są udostępniane, może obejmować także przypadki udostępnienia danych w przyszłości.
3. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o ich udostępnieniu.
4. 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 rozłączalność tych danych.
5. Umożliwia się przekazywanie i wgląd do danych ze zbioru danych upoważnionym do tego służbom (Policja, Straż Miejska, Prokuratura, Sąd) na podstawie pisemnego wniosku kierownika danej jednostki.
6. Dane osobowe ze zbioru „Monitoring wizyjny” przekazywane są na nośnikach zewnętrznych w postaci płyty CD lub DVD wyłącznie upoważnionym do tego służbom (Policja, Straż Miejska, Prokuratura, Sąd) .
7. Przekazanie danych osobowych odbywa się tylko i wyłącznie poprzez osoby do tego uprawnione tj.: Administratora danych.
8. Prowadzony jest odpowiedni rejestr wydawanych nośników.

9. Przekazane dane są dodatkowo kopiowane i zabezpieczane w stacji monitoringu w postaci takiej samej płyty CD lub DVD w celu zabezpieczenia przed jego ewentualnym zniszczeniem, skasowaniem itp.
10. Archiwizowany w pomieszczeniach monitoringu skopiowany nośnik jest odpowiednio zabezpieczony przed dostępem nieuprawnionych osób. Nośnik zostaje odpowiednio opisany (charakter, miejsce i czas zdarzenia), ponumerowany oraz zabezpieczony w szafie zamykanej na klucz. Dostęp do szafy ma Administrator Systemu Monitoringu

XII. Środki techniczne i organizacyjne.

Dane osobowe są chronione przy zastosowaniu następujących zabezpieczeń niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych:

1. Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:
 - 1) budynek i wszystkie pomieszczenia, w których zlokalizowano przetwarzanie danych osobowych zabezpieczone są przed dostępem osób nieuprawnionych
 - 2) dokumentacja papierowa po godzinach pracy osób upoważnionych do jej przetwarzania jest przechowywana w zamykanych biurkach i szafach;
 - 3) przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą wyznaczonej osoby Administratora danych.
2. Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:
 - 1) dla zapewnienia ciągłości działania systemu CCTV służącego do przetwarzania danych osobowych stosuje się sprzęt i oprogramowanie wyprodukowane przez renomowanych producentów oraz zabezpiecza się sprzęt przed awarią zasilania lub zakłóceniami w sieci zasilającej;
3. Przedsięwzięcia w zakresie ochrony teletransmisji danych:
 - 1) w celu ochrony systemu monitoringu służącego do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosuje się zabezpieczenia chroniące przed nieuprawnionym dostępem;
 - 2) transmisja danych osobowych przez publiczną sieć telekomunikacyjną jest zabezpieczona środkami kryptograficznej ochrony danych;
4. Przedsięwzięcia w zakresie środków ochrony w ramach oprogramowania systemów:
 - 1) w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu monitoringu w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło;
 - 2) w przypadku, gdy do uwierzytelnienia użytkowników używa się identyfikatora i hasła, składa się ono z co najmniej 8 znaków, i jest skonstruowane w sposób nie trywialny, w szczególności zawiera małe i duże litery oraz znaki specjalne (np. ?&#%\${*});
 - 3) hasła służące do uwierzytelniania w systemie monitoringu służący do przetwarzania danych osobowych są zmieniane co najmniej raz na 30 dni;
 - 4) w przypadku gdy system CCTV służący do przetwarzania danych osobowych nie wymusza zmiany haseł, użytkownik jest zobowiązany do samodzielnej zmiany hasła po upływie 30 dni.
5. Przedsięwzięcia w zakresie środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych:
 - 1) w celu ochrony zbiorów danych osobowych prowadzonych w systemie CCTV przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych;
 - 2) system powinien zapewniać automatyczne odnotowywanie w systemie informacji o identyfikatorze użytkownika, który wprowadził dane osobowe oraz dacie pierwszego wprowadzenia danych do systemu;
6. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:
 - 1) stosuje się mechanizmy kontroli dostępu użytkowników do zasobów – ogranicza się dostęp do katalogów, ogranicza się wykonywanie poleceń;

- 2) na stacjach roboczych użytkownicy nie posiadają uprawnień do instalowania nieautoryzowanego oprogramowania;
 - 3) stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu monitoringu;
 - 4) kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.
7. Przedsięwzięcia w zakresie środków organizacyjnych.
- 1) wyznaczono Administratora Bezpieczeństwa Informacji;
 - 2) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
 - 3) dostęp do danych osobowych możliwy jest po uzyskaniu zgody do dostępu do danych osobowych wydanej przez upoważnione osoby i w ich obecności;
 - 4) wprowadzono Instrukcję zarządzania systemem monitoringu służącym do przetwarzania danych osobowych;
 - 5) monitoruje się wdrożone zabezpieczenia systemu CCTV

XIII. Zgodność.

1. Niniejsza Polityka oraz dokumenty powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Administratora danych, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Okresowy przegląd Polityki powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Administratora danych oraz są prawnie aktualne w momencie dokonywania przeglądu.
3. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących u Administratora danych.
4. Politykę bezpieczeństwa oraz zmiany Polityki bezpieczeństwa wprowadza się w życie w formie zarządzenia Wójta Gminy Przytyk

XIV. Postanowienia końcowe.

1. W sprawach nieuregulowanych w Polityce 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.
2. Pracownicy Administratora danych zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce. W wypadku uregulowań występujących w innych niż niniejsza Polityka procedurach obowiązujących u Administratora danych, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

Załącznik Nr 2

Do Zarządzenia Nr 57.2013

Wójta Gminy Przytyk

z dnia 15 listopada 2013 r.

Projekt systemu monitoringu wizyjnego w Przytyku

I. Ogólna charakterystyka systemu CCTV

1. Łącznie w systemie monitoringu wizyjnego w Przytyku pracuje obecnie 10 kamer. System monitoringu funkcjonuje w oparciu o dwa systemy:
 - 1) system bezprzewodowy – 5 kamer
 - 2) system przewodowy - 5 kamer (w tym cztery kamery stacjonarne).W/w system monitoringu obsługiwany jest przez przeszkolonych pracowników.

II. Stanowiska operatorskie

1. Pomieszczenia systemu monitoringu te zabezpieczone są przed dostępem osób postronnych. Wideorejestrator znajduje się w zamykanej szafie.

III. Charakterystyka techniczna systemu monitoringu

1. Kamery monitoringu wizyjnego posiadają następujące parametry:
 - 1) Kamery obrotowe (5 szt) DVS-SD, dzień/noc, 600/650 linii, czułość 0,01/001 lux, przetwornik 1,4 SONY, 26 x zoom optyczny, 12 x zoom cyfrowy, 10 tras programowalnych, WDR, temperatura pracy 40 stopniC/+60 stopni C, zabezpieczenie przeciwprzepięciowe do 3000 V, obudowa wandaloodporna, szczelność IP65.
 - 2) Kamera kolorowa wandaloodporna dzień/noc, 650/700 linii, przetwornik 1,3 obiektyw 2,8 – 12 mm, IR z regulacją o zasięgu do 50 m.
2. Rejestrator cyfrowy 16 kanałowy, max 400 kl/s, zaawansowana wideo detekcja, wbudowana karta sieciowa, kompresja H.264, sterowanie przy pomocy myszy i pilota.
3. Kamery systemu monitoringu nie posiadają wbudowanych mechanizmów przetwarzania danych, wykrywania obiektów, identyfikacji, kierunku przemieszczania itp.
4. Kamery systemu CCTV – 5 szt. są kamerami obrotowymi, mającymi możliwość zbliżania i oddalania, przez co szczegółowej obserwacji wybranego obiektu, będącego w rejonie zasięgu danej kamery. Poruszają się automatycznie lub przez operatora. Pozostałe kamery (szt. 5), to kamery stałe bez możliwości przybliżania. Rejestrują one tylko ogólny obraz ulic i teren wokół budynku Urzędu Gminy w Przytyku.

IV. Rozmieszczenia kamer monitoringu

Kamery monitoringu zlokalizowane są na skrzyżowaniach głównych ciągów komunikacyjnych. System monitoringu rozwijany jest w oparciu o analizę miejsc najbardziej zagrożonych. Rozmieszczenie kamer zostało oznaczone na załączonej do dokumentu mapie.

5 kamer stałych – wokół budynku Urzędu Gminy w Przytyku

1 kamera obrotowa Stadion sportowy

1 kamera obrotowa rondo

3 kamery obrotowe rynek.

VI. Sposoby przesyłu wizji.

1. Przesył wizji z poszczególnych kamer odbywa się w dwojaki sposób:
 - 5 kamer stałych – wokół budynku Urzędu Gminy w Przytyku
 - 5 kamer obrotowych – radiowo – kamery zaopatrzone w nadajniki.

VII. Informacje końcowe

1. Polityka bezpieczeństwa przetwarzania danych osobowych monitoringu wizyjnego w Przytyku i stanowi integralną część projektu.
2. Projekt będzie podlegał bieżącej modyfikacji w chwili instalacji nowych kamer, stanowisk, stacji bazowych, zmiany oprogramowania, sposobu przesyłu danych itp.