BIULETYN PRAWNY
UNIWERSYTETU MIKOŁAJA KOPERNIKA W TORUNIU

Rok 2022; poz. 333

ZARZĄDZENIE Nr 198

Rektora Uniwersytetu Mikołaja Kopernika w Toruniu

z dnia 23 grudnia 2022 r.

Regulamin monitoringu wizyjnego

Na podstawie § 52 ust. 3 uchwały Nr 37 Senatu UMK z dnia 16 kwietnia 2019 r. Statut Uniwersytetu Mikołaja Kopernika w Toruniu (Biuletyn Prawny UMK z 2019 r., poz. 120 z późn. zm.)

z a r z ą d z a s i ę, co następuje:

Rozdział 1
Postanowienia ogólne

§ 1

1. Regulamin określa zasady funkcjonowania monitoringu wizyjnego na Uniwersytecie, zasady rejestracji oraz usuwania informacji, a także sposoby ich zabezpieczania i udostępniania.
2. Regulamin obejmuje monitoring stosowany we wszystkich obiektach i na wszystkich terenach części toruńskiej i bydgoskiej Uniwersytetu.
3. Regulamin określa role i zadania poszczególnych jednostek organizacyjnych i komórek administracji Uniwersytetu w zakresie funkcjonowania monitoringu wizyjnego.
4. Użyte w Regulaminie pojęcia oznaczają:
   1) **Uniwersytet** – Uniwersytet Mikołaja Kopernika w Toruniu;
   2) **Administrator Danych Osobowych (ADO)** – Uniwersytet, który decyduje o celach, sposobie oraz zakresie przetwarzania danych osobowych, reprezentowany przez rektora;
   3) **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez ADO na podstawie odrębnych przepisów do sprawowania nadzoru nad przestrzeganiem przepisów i zasad przetwarzania danych osobowych;
   4) **Administrator Systemu Monitoringu (ASM)** – osoba wyznaczona przez kanclerza, odpowiedzialna za całokształt systemu monitoringu wizyjnego oraz realizację Regulaminu;
   5) **Administrator Infrastruktury Monitoringu (AIM)** – osoba wyznaczona przez kanclerza, odpowiedzialna za utrzymanie infrastruktury technicznej monitoringu;
   6) **Administrator Oprogramowania Monitoringu (AOM)** – osoba wyznaczona przez kanclerza w uzgodnieniu z dyrektorem Uniwersyteckiego Centrum

Informatycznego, odpowiedzialna za zarządzanie systemem informatycznym lub systemami informatycznymi obsługującymi monitoring;
7) **Operator Monitoringu (OM)** – osoba zgodnie z zakresem zadań określonym w Regulaminie Organizacyjnym wyznaczona przez ASM do realizacji zadań związanych z obsługą monitoringu w danym obiekcie lub na danym terenie;
8) **monitoring (monitoring wizyjny)** – infrastruktura techniczna wraz z systemami informatycznymi (kamery, rejestratory, oprogramowanie oraz okablowanie) wykorzystywana do zbierania i czasowego przechowywania na nośnikach danych obrazu z określonych obszarów;
9) **Administrator obiektu lub terenu** – kierownik komórki administracji właściwy do administrowania budynkiem lub terenem albo inna upoważniona osoba;
10) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
11) **analiza zgodności** – proces oceny zgodności stosowania monitoringu wizyjnego z wymogami prawa, w tym dotyczących zasadności jego stosowania oraz poszanowania praw i wolności osób fizycznych;
12) **test równowagi** – element analizy zgodności, polegający na wyważeniu praw i wolności osób fizycznych względem celowości stosowania monitoringu wizyjnego w danym miejscu.

5. Załączniki niejawne do Regulaminu stanowią:
1) opis stosowanej infrastruktury monitoringu – załącznik nr 1;
2) opis rozmieszczenia elementów monitoringu – załącznik nr 2;
3) opis stosowanych zabezpieczeń infrastruktury monitoringu przed utratą poufności, dostępności i integralności danych przetwarzanych za jej pomocą – załącznik nr 3.

§ 2

1. Celem zastosowania monitoringu jest zwiększenie bezpieczeństwa osób i mienia znajdujących się na obszarze administrowanym przez Uniwersytet, w szczególności:
1) przeciwdziałanie zachowaniom zagrażających zdrowiu i życiu osób przebywających w budynkach i na terenach administrowanych przez Uniwersytet;
2) przeciwdziałanie zachowaniom przestępczym, wykroczeniom i czynom karalnym oraz innym zagrożeniom bezpieczeństwa;
3) przeciwdziałanie kradzieżom i niszczeniu mienia Uniwersytetu i innych osób;
4) umożliwienie wykrywania zdarzeń wymienionych w pkt 1 do 3 oraz ich sprawców i dostarczanie dowodów.
2. Cel systemu monitoringu wizyjnego wyrażony w ust. 1 jest spełniany z poszanowaniem zasad prywatności, według opracowanej i zaakceptowanej przez Kanclerza koncepcji funkcjonowania.

Rozdział 2
Zasady montażu monitoringu

§ 3

1. System monitoringu składa się z kamer, rejestratorów, serwerów, monitorów oraz okablowania, a także oprogramowania.
2. Elementy systemu monitoringu podlegają, co najmniej raz w roku, okresowym przeglądom i konserwacjom.

3. Monitoring wizyjny nie może rejestrować dźwięku, ale dopuszczalne jest stosowanie technologii, która bez rejestracji i nasłuchu osoby pozwala na podstawie wykrytego dźwięku ustalić rodzaj zagrożenia, np.: wystrzał, wybuch, wzywanie pomocy.
4. Rozmieszczenie i montaż urządzeń monitoringu wizyjnego gwarantują zachowanie poufności, dostępności oraz integralności przetwarzanych informacji na każdym etapie ich przetwarzania przez cały czas funkcjonowania systemu.

§ 4

1. Wybór miejsc objętych monitoringiem oraz punktów instalacji kamer należy do zadań administratorów poszczególnych obiektów i terenów Uniwersytetu.
2. Administratorzy, o których mowa w ust. 1, po dokonaniu wyboru miejsc instalacji kamer, nie później niż w terminie miesiąca przed planowaną instalacją składają wniosek do ASM o akceptację punktów instalacji kamer.
3. Akceptacja ASM następuje po zasięgnięciu opinii:
   1) AOM w terminie 7 dni od dnia otrzymania wniosku;
   2) AIM w terminie 14 dni od dnia przekazania wniosku zaopiniowanego przez AOM.
4. Wniosek, o którym mowa w ust. 2, składa się na formularzu stanowiącym załącznik nr 4 do Regulaminu.

§ 5

1. Przed przystąpieniem do montażu systemu monitoringu wizyjnego w danym obiekcie lub na danym terenie należy przeprowadzić analizę zgodności, w tym test równowagi, analizę ryzyka oraz ocenę skutków przetwarzania dla osób, których dane dotyczą.
2. Analizę zgodności przed montażem systemu monitoringu wizyjnego przeprowadza IOD przy udziale administratorów poszczególnych obiektów.
3. Przy przeprowadzaniu analizy zgodności uwzględnia się przepisy powszechnie obowiązującego prawa, regulacje wewnętrzne i zasady wynikające z Regulaminu.
4. Przeprowadzając test równowagi należy kierować się poszanowaniem prywatności, intymności oraz godności osób, które mogłyby znajdować się w obszarach objętych monitoringiem.
5. AIM oraz AOM wydają opinię i ewentualne zalecenia co do punktów montażu elementów systemu monitoringu wizyjnego w zakresie kompetencji opisanych Regulaminem.

§ 6

1. Instalacja nowego lub modernizacja istniejącego systemu monitoringu wizyjnego muszą być zgodne z Regulaminem oraz przyjętą na Uniwersytecie koncepcją funkcjonowania systemu monitoringu wizyjnego.
2. Za opracowanie i aktualizację koncepcji, o której mowa w ust. 1, jest odpowiedzialny ASM. Koncepcja akceptowana jest przez kanclerza.
3. Uniwersytet może powierzyć opracowanie koncepcji, o której mowa w ust. 1, podmiotowi zewnętrznemu.
4. Zaakceptowana koncepcja funkcjonowania systemu monitoringu wizyjnego podlega aktualizacjom nie rzadziej niż raz na 4 lata.

Rozdział 3
Role i obowiązki

§ 7

1. Administrator Danych Osobowych, jako podmiot decydujący o celach, sposobie i zakresie przetwarzanych danych osobowych odpowiada za prawidłowe i zgodne z prawem funkcjonowanie monitoringu wizyjnego, w tym w zakresie zachowania poufności, dostępności i integralności, przed osobami, których dane dotyczą oraz organami nadzorczymi, w tym Prezesem Urzędu Ochrony Danych Osobowych.
2. Administrator Systemu Monitoringu odpowiada za:
   1) nadzór nad całym systemem monitoringu wizyjnego;
   2) akceptację punktów instalacji kamer;
   3) wyznaczanie, na podstawie Regulaminu, Operatorów Monitoringu;
   4) szkolenia związane z funkcjonowaniem, konserwacją i obsługą systemu monitoringu wizyjnego;
   5) nadzór merytoryczny nad realizacją Regulaminu;
   6) przechowywanie dokumentacji analizy zgodności i testu równowagi oraz nadzór nad pozostałą dokumentacją.
3. Inspektor Ochrony Danych odpowiada za:
   1) nadzór merytoryczny nad zgodnym z prawem funkcjonowaniem monitoringu wizyjnego;
   2) dokonanie z innymi wyznaczonymi osobami uzgodnień dotyczących funkcjonowania monitoringu wizyjnego;
   3) prowadzenie postępowań wyjaśniających i kontrolnych na podstawie odrębnych przepisów;
   4) przeprowadzenie analizy zgodności i testu równowagi;
   5) opiniowanie wniosków dotyczących montażu elementów systemu monitoringu wizyjnego;
   6) wydawanie zaleceń co do stosowanych zabezpieczeń systemu monitoringu wizyjnego.
4. Administrator Infrastruktury Monitoringu odpowiada za:
   1) nadzór nad sprawnym funkcjonowaniem monitoringu od strony technicznej;
   2) przeprowadzanie przeglądów i konserwacji technicznej monitoringu wizyjnego;
   3) nadzór nad prowadzonymi pracami naprawczymi i rozwojowymi;
   4) opiniowanie wniosków dotyczących montażu elementów systemu monitoringu wizyjnego;
   5) prowadzenie dokumentacji dotyczącej infrastruktury monitoringu wizyjnego.
5. Administrator Oprogramowania Monitoringu odpowiada za:
   1) nadzór nad sprawnym funkcjonowaniem systemu lub systemów informatycznych obsługujących monitoring wizyjny;
   2) przeprowadzanie przeglądów i konserwacji, a przede wszystkim aktualizacji systemów o których mowa w pkt.1;
   3) skuteczne zabezpieczenie systemu lub systemów, o których mowa w pkt 1, przed utratą gromadzonych przy ich użyciu informacji, zachowanie poufności, dostępności i integralności poprzez zastosowanie odpowiednich technik i narzędzi;
   4) zabezpieczanie i przygotowywanie, na podstawie Regulaminu, nagrań pochodzących z systemu monitoringu wizyjnego;
   5) udział w analizie zgodności oraz teście równowagi;
   6) opiniowanie wniosków dotyczących montażu elementów systemu monitoringu wizyjnego;

7) prowadzenie dokumentacji dotyczącej systemu lub systemów informatycznych, o których mowa w pkt 1.

6. Uniwersyteckie Centrum Informatyczne odpowiada za współpracę z AOM w zakresie jego działań opisanych w ust. 5 pkt 3.
7. Operator Monitoringu odpowiada za:
   1) bieżącą obsługę monitoringu wizyjnego zainstalowanego w danym budynku lub na danym obszarze;
   2) udostępnianie zgodnie z Regulaminem, za zgodą ASM, nagrań z obsługiwanego monitoringu, jeżeli nie jest ono, z powodów technicznych, możliwe centralnie;
   3) udział w przeprowadzeniu analizy zgodności i testu równowagi;
   4) prowadzenie dokumentacji monitoringu wizyjnego zainstalowanego w danym budynku lub na danym obszarze, w tym szkic sytuacyjny, o którym mowa w § 8 ust. 3;
   5) zgłaszanie wszelkich przejawów nieprawidłowego funkcjonowania monitoringu wizyjnego odpowiednio do AIM w zakresie infrastruktury lub AOM w zakresie systemów informatycznych.

Rozdział 4
Funkcjonowanie i obsługa monitoringu wizyjnego

§ 8

1. Monitoring wizyjny funkcjonuje całodobowo we wszystkich obiektach i terenach administrowanych przez Uniwersytet, które zostały nim objęte.
2. Rejestracji i zapisowi danych podlega tylko obraz z kamer monitoringu.
3. Operator Monitoringu zlokalizowanego w danym budynku lub na danym terenie zobowiązany jest do przygotowania szkicu sytuacyjnego oraz opisu miejsc objętych monitoringiem.
4. Szkic sytuacyjny stanowi informację wewnętrzną, przechowywaną przez Operatora Monitoringu i nie podlega publicznemu dostępowi.
5. Opis miejsc objętych monitoringiem sporządza się według wzoru stanowiącego załącznik nr 2 do Regulaminu, w części dotyczącej zakresu objętego monitoringiem stanowi informację publicznie dostępną u Operatora Monitoringu danego budynku lub terenu.
6. Dane rejestrowane przez monitoring są zapisywane na maksymalny czas wynikający z ustawień i możliwości urządzenia rejestrującego, przy czym nie może on być dłuższy niż 30 dni.
7. Ustęp 6 nie ma zastosowania do danych zabezpieczanych dla potrzeb dochodzenia, ustalenia lub obrony roszczeń oraz w postępowaniach prowadzonych przez organy ścigania.
8. W przypadkach uzasadnionych, w szczególności w przypadku zarejestrowania zdarzenia, o którym mowa w § 2, dane mogą zostać zabezpieczone i zgrane na zewnętrzny nośnik danych.
9. Dane zabezpieczone w sposób opisany w ust. 8 mogą być przechowywane nie dłużej niż jest to wymagane do dochodzenia, obrony lub ustalenia roszczeń bądź przeprowadzenia czynności w postępowaniu prowadzonym przez organy ścigania.

§ 9

1. Dostęp do zgromadzonych danych posiadają:
   1) rektor;
   2) kanclerz;

3) osoby, o których mowa w § 7 – w zakresie wykonywanych obowiązków służbowych;
4) osoby upoważnione przez rektora lub kanclerza – w zakresie upoważnienia.

2. Dostęp do zgromadzonych danych posiadają również:
   1) osoba znajdująca się na nagraniu – w ramach realizacji prawa dostępu do danych osobowych na podstawie art. 15 RODO;
   2) inny podmiot na podstawie odrębnych przepisów.
3. Osoby mające dostęp do danych z monitoringu wizyjnego zobowiązane są do przestrzegania obowiązujących przepisów prawa, procedur, polityki i regulaminów wewnętrznych z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

§ 10

1. Uniwersytet może zlecać firmom zewnętrznym obsługę monitoringu, badanie poprawności jego działania, wykonywanie napraw lub jego rozbudowę i tworzenie dokumentacji w tym zakresie.
2. Jeżeli w trakcie realizacji czynności opisanych w ust. 1, konieczne będzie ujawnienie danych osobowych, niezbędne jest uprzednie podpisanie umowy powierzenia przetwarzania danych osobowych lub umowy poufności.

Rozdział 5
Udostępnianie nagrań

§ 11

1. W przypadku żądania osoby, której dane dotyczą, udostępnia się nagranie z monitoringu w sytuacji, gdy faktycznie znajduje się na nim osoba wnioskująca.
2. W przypadku żądania składanego przez inny podmiot nagranie udostępnia się, gdy wykaże on swój interes prawny i faktyczny.
3. Żądanie udostępnienia nagrania musi określać obszar, z którego pochodzi nagranie oraz przybliżony czas nagrania.
4. O udostępnieniu nagrania decyduje w części toruńskiej kanclerz, a w części bydgoskiej zastępca kanclerza ds. Collegium Medicum.
5. W przypadku wpływu żądania dostępu do nagrania jest ono zabezpieczane poprzez zgranie na zewnętrzny nośnik danych.
6. Przygotowane do udostępnienia nagranie przechowuje się przez maksymalnie 14 dni.
7. Nieodebrane w wyznaczonym czasie nośniki podlegają zniszczeniu w sposób uniemożliwiający dokonanie odczytu.

§ 12

1. Jeżeli żądanie o udostepnienie nagrania z monitoringu nie umożliwia identyfikacji osoby na nagraniu, pozostawia się bez rozpatrzenia.
2. Żądanie osoby, której dane dotyczą jest realizowane bez zbędnej zwłoki, ale nie później niż w ciągu miesiąca od wpływu żądania.
3. W celu ochrony praw i wolności innych osób ich wizerunki muszą być zanonimizowane na udostępnianym nagraniu.
4. Anonimizacji nie stosuje się w przypadku udostępniania nagrań organom ścigania w związku z prowadzonym przez nie postępowaniem.
5. Anonimizację przeprowadza Inspektor Ochrony Danych.
6. Administrator Danych Osobowych zapewnia oprogramowanie komputerowe umożliwiające przeprowadzenie skutecznej anonimizacji na nagraniach wideo.

Rozdział 6
Dostosowanie funkcjonującego monitoringu wizyjnego

§ 13

1. Inspektor Ochrony Danych, przy współpracy innych jednostek organizacyjnych i komórek administracji Uniwersytetu przeprowadzi analizę zgodności funkcjonującego na Uniwersytecie monitoringu wizyjnego pod kątem wymagań Regulaminu.
2. Na podstawie analizy, o której mowa w ust.1, Inspektor Ochrony Danych przygotuje raport przedstawiający rekomendacje w zakresie funkcjonującego monitoringu wizyjnego.
3. Rekomendowane działania mogą polegać między innymi na:
   1) dostosowaniu obecnie funkcjonującego monitoringu wizyjnego do wymogów Regulaminu, poprzez jego modernizację;
   2) likwidacji części monitoringu niespełniającego wymogów Regulaminu lub przyjętej, na podstawie § 6, koncepcji funkcjonowania systemu monitoringu wizyjnego.
4. Raport jest dokumentem wewnętrznym Uniwersytetu i nie podlega publikacji oraz udostępnieniu osobom trzecim.
5. Na podstawie analizy, o której mowa w ust.1, IOD z ASM opracują i przedłożą do zatwierdzenia kanclerzowi harmonogram wdrożenia zaakceptowanych rekomendacji.

Rozdział 7
Postanowienia końcowe

§ 14

1. Minimalne wymagania dla systemu monitoringu wizyjnego określa załącznik nr 5 do Regulaminu.
2. W sprawach monitoringu wizyjnego nieuregulowanych w Regulaminie zastosowanie mają inne przepisy wewnętrzne oraz przepisy powszechnie obowiązującego prawa.

§ 15

1. Regulamin wchodzi w życie z dniem 1 stycznia 2023 r.
2. Analiza, o której mowa w § 13, zostanie przeprowadzona w terminie 6 miesięcy od dnia wejścia w życie Regulaminu.
3. Kanclerz, w drodze zarządzenia, powierzy realizację zadań, o których mowa w § 7 Regulaminu, właściwym osobom, do dnia 15 stycznia 2023 r.

R E K T O R

prof. dr hab. Andrzej Sokala

Załącznik nr 1
do zarządzenia Nr 198 Rektora UMK z dnia 23 grudnia 2022 r.

_____, dn. _____

OPIS STOSOWANEJ INFRASTRUKTURY MONITORINGU

DOKUMENT NIEJAWNY

Teren/Obiekt, którego opis dotyczy:_____

Osoba sporządzająca:_____

Zastosowane rejestratory:
_____
_____
_____

(ilość, producent, model, data instalacji)

Zastosowane dyski twarde:
_____
_____
_____

(ilość, producent, model/numer seryjny, data instalacji)

Zastosowane kamery:
_____
_____
_____

(ilość, producent, model, data instalacji)

Zastosowane okablowanie:
_____
_____
_____

(rodzaj, kategoria, data instalacji)

_____
podpis osoby sporządzającej

Załącznik nr 2
do zarządzenia Nr 198 Rektora UMK z dnia 23 grudnia 2022 r.

_____, dn. _____

OPIS ROZMIESZCZENIA ELEMENTÓW MONITORINGU

DOKUMENT NIEJAWNY

Teren/Obiekt, którego opis dotyczy: _____

Osoba sporządzająca: _____

Część A – rejestratory (wewnętrzna, nie podlega ujawnieniu)

Opis położenia rejestratorów:

_____

_____

_____

Część B – kamery (jawna)

Opis rozmieszczenia kamer:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

podpis osoby sporządzającej

Załącznik nr 3
do zarządzenia Nr 198 Rektora UMK z dnia 23 grudnia 2022 r.

_____, dn. _____

OPIS STOSOWANYCH ZABEZPIECZEŃ INFRASTRUKTURY MONITORINGU PRZED UTRATĄ POUFNOŚCI, DOSTĘPNOŚCI I INTEGRALNOŚCI DANYCH PRZETWARZANYCH ZA JEJ POMOCĄ

DOKUMENT NIEJAWNY

Teren/Obiekt, którego opis dotyczy:_____

Osoba sporządzająca: _____

Opis zabezpieczeń:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
podpis osoby sporządzającej

Załącznik nr 4
do zarządzenia Nr 198 Rektora UMK z dnia 23 grudnia 2022 r.

_____, dn. _____

WNIOSEK O MONTAŻ KAMER SYSTEMU MONITORINGU WIZYJNEGO

Teren/Obiekt, którego wniosek dotyczy: _____

Osoba sporządzająca: _____

Treść wniosku:

Wnoszę o montaż kamery/kamer swoim zasięgiem obejmującej/obejmujących:
_____
_____
_____

Czy wymagana instalacja rejestratora: _____

_____
podpis osoby sporządzającej

Akceptacja Administratora Oprogramowania Monitoringu: _____
_____

Uwagi:
_____
_____

_____
podpis AOM

Akceptacja Administratora Infrastruktury Monitoringu: _____

Uwagi:
_____
_____

_____
podpis AIM

Załącznik nr 5
do zarządzenia Nr 198 Rektora UMK z dnia 23 grudnia 2022 r.

MINIMALNE WYMAGANIA DLA SYSTEMU MONITORINGU WIZYJNEGO

Rozdział I
Minimalne warunki techniczne dla urządzeń rejestrujących

1. Kodowanie: Smart H.265+/H.265/Smart H.264+/H.264/MJPEG/MPEG4.
2. Obsługiwana rozdzielczość kamer: 12 Mpx, 6 Mpx, 5 Mpx, 4Mpx 3 Mpx, 2Mpx1080p, 1.3 Mpx, 720p.
3. Obsługa kamer Onvif.
4. Obsługa HDD do 8TB.
5. Wyjścia Video: 1× HDMI; 1× VGA (HDMI2 3840×2160, VGA 1920×1080).
6. Sieć: 2× RJ-45 (10/100/1000 Mbit/s).
7. Dodatkowe interfejsy: RS485, RS232, port USB.
8. Zasilanie: AC 100~240V 50/60Hz.

Wymaga się, aby rejestracja danych przychodzących z kamer systemu CCTV odbywała się przez nie mniej niż 7 dni.

Rozdział II
Minimalne warunki techniczne dla kamer

1. Kamera kopułowa:
   1) przetwornik 1/2.8” 2 Mpx progressive scan STARVIS CMOS;
   2) efektywna ilość pikseli 1920(H) * 1080(V);
   3) kompresja video H.265+/H.265/H.264+/H.264;
   4) obsługa dwóch strumieni;
   5) 1080p (1920×1080)/1.3 Mpx (1280×960)/720p (1280×720)/D1 (704×576/704×480) /VGA (640×480)/CIF (352×288/352×240);
   6) 2 Mpx przy 25/30 kl./s;
   7) wbudowany obiektyw 2.8 mm, F1.6, czułość 0.002 Lux;
   8) obsługa ICR Dzień/Noc;
   9) wbudowany promiennik IR LED – zasięg do 50 m, Smart IR (dla kamer zewnętrznych);
   10) promiennik podczerwieni (dla kamer zewnętrznych);
   11) funkcje WDR (120dB) 3DNR, AWB, AGC, BLC, HLC Digital Zoom;
   12) wbudowane wejście kart Micro SD max 256GB;
   13) zasilanie DC 12V, PoE (802.3af)/<5.5W Technologia ePoE;
   14) obudowa zewnętrzna IP67, IK10, 1wejścia/1 wyjście alarmowe;
   15) wbudowany Web server.
2. Kamera tubowa:
   1) przetwornik 1/2.8” 2 Mpx progressive scan STARVIS CMOS;
   2) efektywna ilość pikseli 1920(H) * 1080(V);
   3) kompresja video H.265+/H.265/H.264+/H.264;
   4) obsługa dwóch strumieni;
   5) 1080p (1920×1080)/1.3 Mpx (1280×960)/720p (1280×720)/D1 (704×576/704×480) /VGA (640×480)/CIF (352×288/352×240);
   6) 2 Mpx przy 25/30 kl./s;
   7) wbudowany obiektyw 2.7 mm–13.5 mm, czułość 0.002 Lux;
   8) obsługa ICR Dzień/Noc;

9) wbudowany promiennik IR LED – zasięg do 50 m, Smart IR (dla kamer zewnętrznych);
10) promiennik podczerwieni (dla kamer zewnętrznych);
11) funkcje WDR (120dB) 3DNR, AWB, AGC, BLC, HLC Digital Zoom;
12) wbudowane wejście kart Micro SD max 256GB;
13) zasilanie DC 12V, PoE (802.3af)/<10.3W Technologia ePoE;
14) obudowa zewnętrzna IP67, IK10, 1 wejście/1 wyjście alarmowe;
15) wbudowany Web server.

Typ kamer należy potwierdzić na etapie realizacji dokumentacji, poprzez wykonanie wizji lokalnej, ustalenie zasięgu kamer, doświetlenia terenu i widoczności.

Rozdział III
Minimalne warunki położenia urządzeń rejestrujących

1. Urządzenie nie może być dostępne dla osób postronnych.
2. Urządzenie musi być zamontowane w sposób ograniczający podatność na uszkodzenia mechaniczne i elektromagnetyczne, a także wilgoć.
3. Urządzenie musi pracować w sieci LAN zabezpieczonej przed dostępem z zewnątrz.
4. Urządzenie musi pracować w sieci elektroenergetycznej zabezpieczonej przed przepięciami, chwilowymi zanikami napięcia i innymi niekorzystnymi zjawiskami.

Rozdział IV
Minimalne warunki dla punktów instalacji kamer

1. Instalacja kamer poprzedzona jest przeprowadzeniem wizji lokalnej i sporządzeniem stosownej dokumentacji.
2. Wysokość montażu kamer winna mieścić się w przedziale między 3 a 4 metry wysokości od podłoża, o ile warunki techniczne na to pozwalają.
3. Punkty kamerowe powinny być zamontowane w taki sposób, aby ukierunkowanie obiektywów kamer pozwalało na obserwację tylko obszaru będącego w posiadaniu Uniwersytetu.
4. Przy projektowaniu punktów kamerowych należy wziąć pod uwagę zakaz rejestracji obrazu i dźwięku w miejscach naruszających intymność i prywatność – w pomieszczeniach sanitarnych, szatniach, stołówkach, pomieszczeniach socjalnych itp.
5. Zakaz rejestracji dźwięku tyczy się wszystkich kamer zainstalowanych w systemie.

Rozdział V
Minimalne warunki dla systemów informatycznych

1. Systemy informatyczne dedykowane do obsługi monitoringu wizyjnego muszą gwarantować pracę na indywidualnych kontach użytkowników.
2. System musi być zabezpieczony unikatowym loginem i hasłem dla każdego użytkownika.
3. System musi dawać możliwość przypisywania zróżnicowanych ról, z różnym zakresem uprawnień.
4. System służący do przygotowania nagrania do udostępnienia musi gwarantować możliwość anonimizowania osób w sposób zautomatyzowany.

Rozdział VI
Minimalne warunki techniczne dla zapewnienia poufności i dostępności danych

1. Kamery muszą mieć możliwość zaznaczania obszarów wyłączonych z nagrywania.
2. Umiejscowienie monitorów służących do podglądu obrazu z systemu monitoringu musi gwarantować brak możliwości dostępu do nich przez osoby postronne.
3. Urządzenia rejestracyjne muszą spełniać warunki przechowywania nagrań przez wyznaczony okres.

Rozdział VII
Zasady informowania o stosowaniu monitoringu wizyjnego

1. Każdy obiekt/teren objęty monitoringiem musi być odpowiednio oznaczony.
2. Oznaczenie musi zawierać minimum następujące informacje:
   1) obiekt/teren monitorowany;
   2) informację o administratorze danych;
   3) informacje o celach przetwarzania;
   4) podstawowe prawa osób, których dane dotyczą;
   5) dane kontaktowe inspektora ochrony danych;
   6) odesłanie do pełnej treści informacji o przetwarzaniu danych osobowych.
3. Oznaczenie obiektów:
   1) budynki muszą być oznaczone w miejscu każdego wejścia do budynku;
   2) oznaczenie musi być widoczne i czytelne;
   3) w przypadku gdy nastąpiło oznaczenie przy wejściu na teren objęty monitoringiem, a do budynku nie ma innego dojścia, na wejściu do budynku wystarczy zamieścić znak o treści „budynek monitorowany”.
4. Oznaczenie terenów:
   1) teren musi być oznakowany w sposób umożliwiający zapoznanie się z informacją przez osobę, która ma zamiar wejść na obszar objęty monitoringiem;
   2) oznaczenie musi być widoczne i czytelne;
   3) w przypadku wjazdów oznaczenie musi być widoczne i czytelne z pozycji osób znajdujących się w pojeździe.