

POLITECHNIKA POZNAŃSKA

DZIAŁ BEZPIECZEŃSTWA

REGULAMIN

FUNKCJONOWANIA MONITORINGU WIZYJNEGO
w POLITECHNICE POZNAŃSKIEJ



ZATWIERDZAM

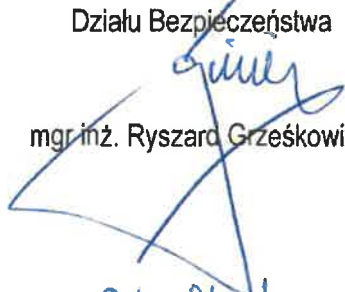

KANCLERZ
Politechniki Poznańskiej
dr Łukasz KALUPA

REGULAMIN

FUNKCJONOWANIA MONITORINGU WIZYJNEGO

w POLITECHNICE POZNAŃSKIEJ

KIEROWNIK
Działu Bezpieczeństwa


mgr inż. Ryszard Grześkowiak

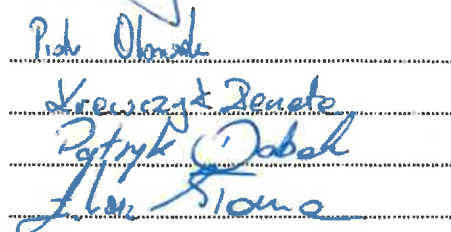
UZGODNIONO:

Inspektor Ochrony Danych:

Inspektor Bezpieczeństwa Informacji:

Administrator Systemu Teleinformatycznego ASK „Z” PP:

Radca Prawny PP:


Piotr Obrowski
Krzysztof Benato
Piotr Dabek
Jan Sionko

SPIS TREŚCI	strona
§ 1. Zapisy ogólne	- 7
§ 2. Cel monitoringu	- 8
§ 3. Obszar i zasady monitoringu	- 9
§ 4. Procedura instalacji i integracji urządzeń monitoringu wizyjnego	- 11
§ 5. Uprawnienia do przetwarzania danych i dostęp do nagrań	- 12
§ 6. Ochrona danych osobowych	- 12
§ 7. Zabezpieczenie i przechowywanie nagrań	- 13
§ 8. Procedura wnioskowania o zabezpieczenie nagrań	- 13
§ 9. Postanowienia końcowe	- 14
Załączniki:	
Nr 1. WNIOSEK – formularz zgłoszeniowy	- 17
Nr 2. WNIOSEK o zabezpieczenie/udostępnienie nagrań z monitoringu wizyjnego	- 19
Nr 3. Klauzula Informacyjna	- 21

§ 1. Zapisy ogólne

1. Niniejszy Regulamin określa:
 - 1) cel i zasady funkcjonowania systemu monitoringu wizyjnego w Politechnice Poznańskiej zwanej dalej "Uczelnią";
 - 2) lokalizację urządzeń monitorujących;
 - 3) zasady instalacji i integracji systemu monitoringu wizyjnego z Uczelnianym Centrum Monitoringu;
 - 4) zasady zapisu obrazu i jego przechowywania;
 - 5) zasady udostępniania nagrań z monitoringu wizyjnego.
2. Administratorem systemu monitoringu wizyjnego jest Politechnika Poznańska.
3. Ilekroć w Regulaminie jest mowa o:
 - 1) **Monitoringu wizyjnym** – należy przez to rozumieć system rejestracji obrazu wykorzystywany przez Uczelnię w celu zapewnienia bezpieczeństwa osób i ochrony mienia;
 - 2) **Systemie monitoringu wizyjnego (CCTV)** – należy przez to rozumieć infrastrukturę techniczną monitoringu Uczelni;
 - 3) **Uczelniane Centrum Monitoringu (UCM)** – wydzielone miejsce na terenie Uczelni, wyposażone w systemy monitoringu i infrastruktury bezpieczeństwa, w którym wyznaczeni pracownicy Działu Bezpieczeństwa oraz Straży Akademickiej prowadzą bieżący nadzór nad sytuacją na terenie Uczelni oraz koordynują działania Straży Akademickiej;
 - 4) **Nagraniach** – należy przez to rozumieć zapis obrazu, danych lokalizacyjnych GPS oraz danych opisowych zgromadzonych w systemie monitoringu;
 - 5) **Udostępnienie nagrania z systemu CCTV** – należy przez to rozumieć przekazanie kopii nagrania lub umożliwienie trwałego pozyskania danych z monitoringu podmiotowi uprawnionemu na podstawie przepisów prawa, w szczególności Policji, prokuraturze, sądom lub innym organom prowadzącym postępowanie;
 - 6) **Wgląd do nagrania** – należy przez to rozumieć umożliwienie osobie, której dane dotyczą lub która uczestniczyła w zdarzeniu objętym monitoringiem, zapoznania się z nagraniem bez przekazywania kopii materiału i bez możliwości jego samodzielnego utrwalenia lub rozpowszechniania;
 - 7) **Sekcja Techniczna** – należy przez to rozumieć wyznaczonych pracowników Działu Bezpieczeństwa Politechniki Poznańskiej, odpowiedzialnych za:
 - a) **utrzymanie sprawności technicznej systemu monitoringu wizyjnego** (zapewnienie ciągłej sprawności kamer, rejestratorów, serwerów, macierzy utrzymywanych w Dziale Bezpieczeństwa i pozostałych elementów systemu, bieżące usuwanie awarii i usterek, prowadzenie konserwacji okresowych zgodnie z dokumentacją producentów i obowiązującymi procedurami, kontrolę poprawności działania urządzeń oraz jakości obrazu);
 - b) **eksploatację infrastruktury CCTV** (zarządzanie urządzeniami i ich konfiguracją, utrzymanie we współpracy z Działem Obsługi i Eksploatacji infrastruktury transmisyjnej wykorzystywanej przez system, kontrola zasilania podstawowego i awaryjnego urządzeń, monitorowanie pojemności pamięci masowych i poprawności archiwizacji nagrań, określanie lokalizacji kamer i uzasadnianie ich montażu, administrowanie systemem monitoringu w zakresie użytkowników i uprawnień, udostępnianie nagrań uprawnionym podmiotom, prowadzenie postępowań wyjaśniających);

- c) **rozwój i modernizację systemu** (przygotowywanie koncepcji rozbudowy systemu, udział w opracowywaniu dokumentacji technicznej, szacowanie kosztów inwestycji, nadzór techniczny nad realizacją nowych instalacji oraz odbiór wykonanych prac);
- d) **wsparcie użytkowników** (realizacja zgłoszeń dotyczących usterek, udzielanie wsparcia jednostkom organizacyjnym w zakresie funkcjonowania systemu, analiza potrzeb dotyczących nowych punktów kamerowych);
- e) **dokumentację** (aktualizacja dokumentacji technicznej, schematów i konfiguracji, prowadzenie rejestru awarii, napraw i przeglądów, przygotowywanie informacji dotyczących stanu technicznego systemu);
- f) **współpracę z wykonawcami** (nadzór nad firmami serwisowymi, odbiór prac konserwacyjnych i inwestycyjnych, weryfikacja jakości wykonywanych usług, zgłaszanie reklamacji gwarancyjnych);
- g) **zapewnienie bezpieczeństwa technicznego** (wykonywanie kopii konfiguracji systemu, aktualizacja oprogramowania urządzeń, eliminowanie podatności technicznych we współpracy z Działem Obsługi i Eksploatacji oraz Inspektorem Bezpieczeństwa Informacji, dbanie o zgodność konfiguracji z obowiązującymi standardami bezpieczeństwa);
- h) **planowanie budżetu** (przygotowywanie danych do planów rzeczowo-finansowych dotyczących utrzymania i rozwoju CCTV, określanie potrzeb zakupowych, planowanie wymiany urządzeń kończących cykl życia).

§ 2. Cel monitoringu

1. Monitoring wizyjny prowadzony jest w celu:
 - 1) zapewnienia bezpieczeństwa studentów, pracowników oraz innych osób przebywających na terenie Uczelni;
 - 2) ochrony mienia Uczelni;
 - 3) przeciwdziałania naruszeniom porządku publicznego i bezpieczeństwa na terenie Uczelni;
 - 4) dokumentowania zdarzeń związanych z zagrożeniem życia, zdrowia, mienia, a także innych zdarzeń, których obowiązek rejestracji lub kontroli wynika z przepisów odrębnych, w szczególności dotyczy to przeprowadzania i dokumentowania egzaminów;
 - 5) wspomagania działań podejmowanych przez Straż Akademicką Uczelni;
 - 6) zabezpieczenia materiału dowodowego na potrzeby postępowań prowadzonych na podstawie przepisów prawa.
2. Monitoring nie może być wykorzystywany do:
 - 1) stałej kontroli efektywności pracy pracowników;
 - 2) ingerowania w prywatność osób w zakresie wykraczającym poza cele wskazane w ust. 1;
 - 3) obserwacji pomieszczeń, w których mogłoby dojść do naruszenia godności lub dóbr osobistych osób przebywających na terenie Uczelni, chyba że obowiązujące przepisy prawa stanowią inaczej.
3. Niniejszy Regulamin stanowi uszczegółowienie oraz rozwinięcie postanowień zawartych w Regulaminie Pracy Politechniki Poznańskiej w zakresie zasad stosowania monitoringu wizyjnego na Uczelni wprowadzonych na podstawie art. 22 ⁽²⁾ ustawy z dnia 20 lipca 1974 r. Kodeks Pracy (Dz.U. z 2025 r., poz. .277 z późn. zm).
4. Podstawy prawne wdrożenia systemu monitoringu wizyjnego to przepisy prawa powszechnie obowiązującego oraz wewnętrznych aktów prawnych, w szczególności:
 - 1) art. 50 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz.U. z 2024 r., poz.1571 z późn. zm);
 - 2) Ustawa z dnia 22 sierpnia 1997 o ochronie osób i mienia;

- 3) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

§ 3. Obszar i zasady monitoringu

1. Zasady monitorowania.

- 1) Monitoring nie może naruszać prywatności osób przebywających na terenie Uczelni, a zasady ochrony danych osobowych muszą być ściśle przestrzegane.
- 2) **Kamery mogą być instalowane** zgodnie z § 2 ust. 1 obejmując między innymi:
 - a) laboratoria badawcze i dydaktyczne – w celu ochrony kosztownego sprzętu, zwłaszcza w miejscach, gdzie przechowywane są urządzenia o dużej wartości. Kamery mogą chronić wyposażenie przed kradzieżą, uszkodzeniem lub nieautoryzowanym dostępem;
 - b) pomieszczenia z drogocennym sprzętem – np. sale komputerowe, serwerownie, pracownie specjalistyczne, biblioteki (z wyłączeniem obszarów, które mogą obejmować prywatność użytkowników);
 - c) magazyny sprzętu – wszelkie pomieszczenia, w których przechowywany jest sprzęt, materiały laboratoryjne, urządzenia uczelniane;
 - d) korytarze, ciągi komunikacyjne, przestrzenie wspólne – miejsca, które są ogólnodostępne, a monitoring może zapewnić bezpieczeństwo osobom poruszającym się po Uczelni (np. na wypadek incydentów kryminalnych);
 - e) wejścia i wyjścia z budynków – monitoring w okolicach wejść do budynków, w tym przy drzwiach głównych, bocznych, na korytarzach, w holach wejściowych;
 - f) miejsca postojowe i inne zewnętrzne przestrzenie Uczelni – tereny parkingowe, podjazdy, chodniki wokół budynków, które mogą być monitorowane w celu zapewnienia bezpieczeństwa pojazdów oraz osób poruszających się po terenie Uczelni;
 - g) miejscach w których wykonywane są prace administracyjno-biurowe związane z operacjami / transakcjami finansowymi, przechowywaniem danych podlegających szczególnej ochronie (np. sekretariaty, dziekanaty, kancelarie, archiwa).
- 3) Monitoring nie obejmuje: pomieszczeń udostępnianych zakładowej organizacji związkowej, pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 2.ust. 1. i nie narusza to godności oraz innych dóbr osobistych.
- 4) Monitoring pozostaje aktywny przez całą dobę.
2. Obraz z kamer CCTV jest przesyłany do Uczelnianego Centrum Monitoringu (UCM), gdzie operatorzy w czasie rzeczywistym dokonują obserwacji terenu i obiektów Uczelni, odbierają i analizują sygnały oraz podejmują decyzję w celu usunięcia zagrożeń bezpieczeństwa lub ich minimalizacji.
3. Kamery i urządzenia niepodłączone do ogólnouczelnianego systemu CCTV mogą być używane do prowadzenia monitoringu w Uczelni po uzyskaniu pisemnej ZGODY Kanclerza wydanej na podstawie złożonego wniosku określonego w § 4 ust. 1 oraz wydanych opinii.

4. Kamery oraz urządzenia wchodzące w skład systemu monitoringu Uczelni oraz kamery i urządzenia niepodłączone do ogólnouczelnianego systemu CCTV utrzymywane są z zastosowaniem środków organizacyjnych i technicznych zapewniających odpowiedni poziom bezpieczeństwa, obejmujących w szczególności:
 - 1) nagrania mogą być przechowywane wyłącznie w lokalizacji zaakceptowanej przez Dział Obsługi i Eksploatacji, jednocześnie nie dopuszcza się przetwarzania nagrań monitoringu na niezabezpieczonych zewnętrznych nośnikach danych, zewnętrznych usługach chmurowych oraz na innych niezabezpieczonych przed nieuprawnionym dostępem urządzeniach, bez uzyskania zgody Kanclerza Politechniki Poznańskiej;
 - 2) ograniczenie dostępu administracyjnego do urządzeń i aplikacji wyłącznie do upoważnionych osób;
 - 3) stosowanie indywidualnych kont użytkowników zabezpieczonych silnymi hasłami oraz, jeśli jest to technicznie możliwe, uwierzytelniania wieloskładnikowego;
 - 4) szyfrowanie transmisji danych podczas sieciowego dostępu do urządzeń i aplikacji zarządzających;
 - 5) rejestrowanie logów dostępu, zmian konfiguracji oraz prób logowania;
 - 6) stosowanie zabezpieczeń sieciowych, w szczególności segmentacji sieci oraz ograniczeń dostępu z wykorzystaniem zapór sieciowych (firewall);
 - 7) utrzymywanie aktualnego oprogramowania urządzeń oraz aplikacji zarządzających poprzez regularne instalowanie dostępnych aktualizacji bezpieczeństwa;
 - 8) konfigurację urządzeń obejmującą w szczególności zmianę fabrycznych haseł dostępu oraz wyłączenie domyślnie aktywnych usług i funkcji, które nie są wykorzystywane (np. zdalnego dostępu);
 - 9) prawidłową konfigurację czasu, strefy czasowej oraz synchronizacji czasu w celu zapewnienia wiarygodności i integralności nagrań;
 - 10) stosowanie procedur bezpiecznego wycofania urządzeń z eksploatacji, obejmujących trwałe usunięcie danych oraz przywrócenie ustawień fabrycznych, jeżeli jest to uzasadnione.
5. Osoby/a odpowiedzialna za przetwarzanie i udostępnianie danych oraz prowadzenie wymaganej dokumentacji w zakresie systemu monitoringu funkcjonującego poza CCTV, wskazana we wniosku określonym w § 4 ust.1, zapewnia prawidłowe funkcjonowanie systemu monitoringu, w tym kamer i urządzeń rejestrujących, poprzez ich właściwą konfigurację, aktualizację oraz okresową weryfikację poprawności konfiguracji, parametrów pracy i procesu rejestracji obrazu. Ponadto nadzoruje właściwe oznakowanie obszaru objętego monitoringiem oraz weryfikuje, czy monitoring jest wykorzystywany wyłącznie w celu i zakresie określonych na etapie jego uruchamiania.
6. Przełożony wnioskodawcy wskazany we wniosku określonym w § 4 ust.1, odpowiada za zapewnienie organizacyjnych warunków funkcjonowania systemu monitoringu zgodnie z niniejszym Regulaminem.

§ 4. Procedura instalacji i integracji urządzeń monitoringu wizyjnego

1. **Wniosek**¹ - formularz zgłoszeniowy dot. monitoringu wizyjnego - montaż / instalacja / zgłoszenie / włączenie urządzeń CCTV do systemu monitoringu wizyjnego składany jest do Kanclerza, Politechniki Poznańskiej poprzez Dział Bezpieczeństwa (załącznik nr 1 do niniejszego Regulaminu).
2. Wniosek - formularz zgłoszeniowy powinien zawierać w szczególności:
 - 1) szczegółowe uzasadnienie (np. zabezpieczenie sprzętu badawczego);
 - 2) wskazanie lokalizacji kamer;
 - 3) czas pracy urządzeń (całodobowo lub w określonych godzinach);
 - 4) udzielone zgody ²;
 - 5) wskazanie osób upoważnionych do przeglądania / rejestracji / udostępniania zapisu danych z monitoringu;
 - 6) wskazanie źródła finansowania:
 - a) środki wydziałowe lub instytutowe, jeśli zakup jest zgodny z planem finansowym wydziału/instytutu;
 - b) środki uczelniane (np. budżet Kanclerza) w przypadku większych inwestycji lub konieczności sfinansowania z innych funduszy (np. fundusze przeznaczone na bezpieczeństwo).
 - 7) wnioskodawca do Wniosku dołącza:
 - a) opinię techniczną z określeniem parametrów urządzeń, oprogramowania, możliwości montażu urządzeń oraz szacunkowymi kosztami ³,
 - b) opinię Inspektora Ochrony Danych (IOD) z uwzględnieniem:
 - podstawy prawnej przetwarzania danych,
 - oceny zgodności celu przetwarzania (czy cel instalacji kamer jest konkretny, wyraźny i zgodny z prawem, czy monitoring nie narusza zasady minimalizacji – tzn. czy kamery obejmują tylko niezbędne obszary, czy zapewniono transparentność i obowiązek informacyjny tzn. czy zapewnione zostaną właściwe informacje dla osób, których dane dotyczą zgodnie z art. 13 RODO, np. tabliczki informacyjne).
3. Monitoring funkcjonujący w Uczelni, poza ogólnouczelnianym systemem CCTV, należy zgłosić do Działu Bezpieczeństwa w celu określenia możliwości integracji.
4. Etapy instalacji urządzeń:
 - 1) Zakup sprzętu.

Zakupy dokonywane są zgodnie z wewnętrzną procedurą zakupową Uczelni. Należy przestrzegać regulacji prawnych, w tym prawa o zamówieniach publicznych. Opis przedmiotu

¹ Wniosek – formularz zgłoszeniowy należy składać wg układu hierarchicznego określonego w strukturze Uczelni

² jw.

³ opinię wystawia wyznaczony pracownik Sekcji Technicznej Działu Bezpieczeństwa w porozumieniu z wyznaczonym pracownikiem Działu Obsługi i Eksploatacji w zakresie akceptacji miejsca przechowywania nagrań.

zamówienia przygotowuje Sekcja Techniczna Działu Bezpieczeństwa. Pozostałe procedury wykonuje wnioskodawca z Działem Zamówień Publicznych.

2) Montaż urządzeń:

- a) pojedyncze kamery montuje Sekcja Techniczna Działu Bezpieczeństwa;
- b) dla większej liczby urządzeń montaż zleca się firmie zewnętrznej, wyłonionej zgodnie z wewnętrzną procedurą zakupową Uczelni.

3) Integracja urządzeń z infrastrukturą techniczną monitoringu Uczelni ⁴: po zamontowaniu kamery należy przeprowadzić jej konfigurację, integrację z systemem CCTV, konfigurację w systemie zarządzania monitoringiem, weryfikację poprawności działania oraz aktualizację dokumentacji technicznej i ewidencyjnej. Urządzenie może zostać przekazane do eksploatacji po pozytywnym zakończeniu testów funkcjonalnych.

§ 5. Uprawnienia do przetwarzania danych i dostęp do nagrań

1. Dostęp do nagrań.

Dostęp do zapisów z monitoringu mają wyłącznie osoby upoważnione:

- 1) Administrator Danych Osobowych Uczelni (Rektor),
- 2) Inspektor Ochrony Danych Uczelni,
- 3) Kierownik Działu Bezpieczeństwa,
- 4) oraz inne osoby zatrudnione:
 - a) w Dziale Bezpieczeństwa odpowiedzialne za przeglądanie, zabezpieczanie, udostępniania nagrań oraz za serwisowanie sprzętu i systemów CCTV,
 - b) w innych jednostkach organizacyjnych Uczelni na podstawie ważnego upoważnienia wydanego przez Administratora Danych Osobowych, po przeszkoleniu w zakresie ochrony danych osobowych.

2. Upoważnienie/a do przetwarzania danych osobowych zawartych w systemie monitoringu wizyjnego:

- 1) przygotowuje Administrator Danych Osobowych,
- 2) upoważnione osoby podpisują zobowiązanie do przestrzegania zasad ochrony danych osobowych oraz procedur bezpieczeństwa.
- 3) każde logowanie do systemu oraz operacje wykonywane na nagraniach podlegają rejestracji w dziennikach systemowych.

§ 6. Ochrona danych osobowych

1. Zasady ochrony danych.

Administrator systemu monitoringu wizyjnego spełnia obowiązki wynikające z art. 13 RODO i informuje osoby objęte monitoringiem o przetwarzaniu ich danych osobowych (w tym celu

⁴ § 4 ust. 4. pkt 3 nie dotyczy urządzeń funkcjonujących poza systemem CCTV

wywieszana jest warstwowa klauzula informacyjna). Szczegółowe informacje dotyczące przetwarzania danych osobowych znajdują się na stronie internetowej Uczelni.

2. Prawa osób objętych monitoringiem:

- 1) Prawo do dostępu do nagrań;
- 2) Prawo do żądania usunięcia danych;
- 3) Prawo do zgłoszenia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§ 7. Zabezpieczenie i przechowywanie nagrań

1. Okres przechowywania.

- 1) Nagrania z systemu monitoringu wizyjnego przechowywane są przez okres nie dłuższy niż **14 dni** od dnia ich zarejestrowania, zgodnie z zasadą minimalizacji okresu retencji, o której mowa w art. 5 ust. 1 lit. e RODO, chyba że:
 - a) stanowią dowód w postępowaniu;
 - b) Administrator Danych powziął wiadomość, iż mogą stanowić dowód w postępowaniu.
- 2) W przypadkach określonych w pkt. 1 ust. 1) lit. a i b termin przechowywania ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
- 3) Po upływie wskazanego okresu nagrania są automatycznie nadpisywane lub bezpowrotnie usuwane w sposób uniemożliwiający ich odzyskanie.
- 4) Ustalony, jednolity okres przechowywania nagrań obowiązuje we wszystkich jednostkach organizacyjnych Uczelni. Odstępstwa od tej zasady są niedopuszczalne bez uprzedniej rekomendacji Inspektora Ochrony Danych, zgody wydanej przez Kanclerza bądź Rektora PP, chyba że przepisy odrębne stanowią inaczej.

2. Zabezpieczenie przed dostępem osób nieuprawnionych.

Nagrania muszą być przechowywane w sposób zapewniający ich bezpieczeństwo i uniemożliwiający nieautoryzowany dostęp.

3. Przedłużenie przechowywania.

W przypadku, gdy nagranie jest dowodem w postępowaniu administracyjnym lub sądowym, okres przechowywania może zostać przedłużony do zakończenia postępowania.

§ 8. Procedura wnioskowania o zabezpieczenie nagrań

1. Wniosek o zabezpieczenie nagrania.

- 1) W przypadku potrzeby zabezpieczenia nagrania, osoba fizyczna lub organ wnoszący o zabezpieczenie musi złożyć odpowiedni wniosek w Dziale Bezpieczeństwa przekazując dane określone w załączniku nr 2 do niniejszego Regulaminu.
- 2) Wniosek podlega rejestracji i archiwizacji.

2. Procedura wnioskowania.

Wniosek powinien zawierać dokładną datę, godzinę i miejsce zdarzenia, które zostało zarejestrowane. Wniosek należy złożyć w terminie do max. 14 dni od zaistniałego zdarzenia.

3. Udostępnianie nagrań:

- 1) nagrania mogą być udostępniane tylko na pisemny wniosek uprawnionych organów państwowych na podstawie przepisów prawa, na żądanie uprawnionych organów;
- 2) w uzasadnionych przypadkach, np. w celu wyjaśnienia zdarzeń, zapis może być udostępniony do wglądu zainteresowanej osobie, jednak zawsze z zachowaniem anonimizacji innych osób;
- 3) udostępniane nagranie lub nośnik danych, na którym je zamieszczono, podlegają szyfrowaniu;
- 4) operacje zgrywania nagrań podlegają ewidencjonowaniu, poprzez odnotowanie daty, godziny, nazwy pliku i osoby wykonującej operacji zapisu nagrania.

§ 9. Postanowienia końcowe

1. Obowiązek informacyjny.

- 1) Uczelnia informuje o stosowaniu monitoringu poprzez:
 - a) oznaczenia graficzne;
 - b) Zarządzenie Rektora, w którym następuje publikacja Regulaminu;
 - c) klauzulę informacyjną dotyczącą przetwarzania danych osobowych, która określa w szczególności:
 - Administratora Danych;
 - cele i podstawy przetwarzania danych;
 - okres przechowywania danych;
 - prawa osób, których dane dotyczą;
 - dane kontaktowe Inspektora Ochrony danych.

2. Bezpieczeństwo IT.

Nagrania muszą być chronione przed nieautoryzowanym dostępem, usunięciem, uszkodzeniem, kradzieżą oraz innymi zagrożeniami cybernetycznymi, w celu zapewnienia poufności, integralności i dostępności informacji.

3. Wnioski i prośby.

- 1) W przypadku jakichkolwiek wątpliwości lub potrzeby zgłoszenia problemów związanych z instalacją, użytkowaniem urządzeń CCTV, należy kontaktować się z Działem Bezpieczeństwa mailowo na adres kontrola.dostepu@put.poznan.pl
- 2) Zgodnie z obowiązującymi przepisami prawa (w szczególności ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 – RODO), **monitoring wizyjny może być stosowany wyłącznie na podstawie odpowiednich przepisów oraz za zgodą uprawnionych organów Uczelni, w szczególności Rektora.** Nielegalne lub samowolne rozmieszczenie kamer monitoringu może skutkować:
 - a) odpowiedzialnością dyscyplinarną,
 - b) odpowiedzialnością służbową lub karną,

c) koniecznością natychmiastowego demontażu systemu CCTV.

Lukasz Słoma

RADCA PRAWNY

.....
miejscowość, data

Kanclerz
Politechniki Poznańskiej
poprzez
Dział Bezpieczeństwa

.....
nr wniosku

.....
miejscowość data wpływu

WNIOSEK – formularz zgłoszeniowy

1. Nazwa jednostki wnioskującej

2. Nazwa systemu

Monitoring Wizyjny - montaż / instalacja / zgłoszenie / włączenie ' urządzeń CCTV do systemu monitoringu wizyjnego Politechniki Poznańskiej

3. Opis zgłoszenia - czas pracy urządzeń

W opisie uwzględnić: zakup kamery IP typu ..., zakres wymaganych prac, w tym np. zakup materiałów montażowych, wykonanie trasy kablowej i montażu kamery, konfiguracja kamery, integracja z systemem CCTV, testy funkcjonalne, dokumentacja powykonawcza.

Czas pracy urządzeń: 24h/d bądź inny w przypadku monitoringu funkcjonującego poza CCTV .

4. Lokalizacja

Obiekt: **pomieszczenie/a:** **Miejsce zapisu danych:**

5. Szczegółowe UZASADNIENIE:

W uzasadnieniu uwzględnić: jakie uwarunkowania generują potrzebę realizacji przedsięwzięcia, w tym m.in. wpływ na bezpieczeństwo życia i zdrowia, wymagania prawne, wpływ na ciągłość działania, ryzyko wystąpienia incydentów oraz potencjalne skutki finansowe i straty wynikające z ich wystąpienia.

6. Osoby odpowiedzialne za przetwarzanie i udostępnianie danych oraz prowadzenie wymaganej dokumentacji wg obowiązków określonych w § 3. ust. 4 - 5

Imię Nazwisko - stanowisko – jo – tel. kontakt. (dotyczy wyłącznie systemu funkcjonującego poza syst. CCTV)

7. Orientacyjne koszty (Wnioskodawca wypełnia razem z przedstawicielem Sekcji Technicznej)

	element	ilość	cena jedn. PLN	wartość brutto
poz.1	Zakup kamery IP typu HIK (4–8 MP, PoE)	1	1 200, 00 zł	1 200,00
poz.2	Materiały montażowe (uchwyty, puszka, złącza, peszle, elementy mocujące)	1 kpl	400, 00 zł	400,00
poz.3	Przewód UTP kat. 5e/6 wraz z zakończeniami	1 kpl	400, 00 zł	400,00
poz.4	Wykonanie trasy kablowej i montaż kamery	usługa	800, 00 zł	800,00
poz.5	Konfiguracja kamery (adresacja IP, aktualizacja oprogramowania, parametry obrazu)	usługa	Sekcja Techniczna	
poz.6	Integracja z systemem monitoringu wizyjnego PP (rejestrator/VMS, nadanie uprawnień, testy)	usługa	Sekcja Techniczna	

poz.7	Uruchomienie, testy funkcjonalne i odbiór techniczny	usługa	Sekcja Techniczna	
poz.8	Dokumentacja powykonawcza i aktualizacja dokumentacji systemu monitoringu	usługa	200, 00 zł	200,00
poz.9				
poz.10				
			Koszty razem	3 000,00

8. Wskazanie źródła finansowania (MPK, ŻF, K. alokacji, Projekt, Rok budżetowy)

9. Wnioskodawca (tytuł imię NAZWISKO - stanowisko - jednostka organizacyjna – numer telefonu)

podpis

10. Przełożony Wnioskodawcy (tytuł imię NAZWISKO - stanowisko - jednostka organizacyjna – numer telefonu)

Wniosek akceptuję i przesyłam do dalszego procedowania

podpis

OPINIE

1. Opinia Techniczna (wystawia Sekcja Techniczna oraz Dział Obsługi i Eksploatacji. Opinia obejmuje min.: parametry techniczne urządzeń, możliwości montażu, możliwości włączenia do UCM, szacunkowe koszty, określenie priorytetu uwzględniające szczegółowe uzasadnienie, akceptację miejsca przechowywania nagrań, itp.)

Określenie priorytetu	priorytet I. - krytyczny	priorytet II. - istotny	priorytet III. - rozwojowy

podpis osoby upoważnionej z Sekcji Technicznej

Akceptuję miejsce zapisu danych

podpis osoby upoważnionej z Działu Obsługi i Eksploatacji

2. Opinia Inspektora Ochrony Danych (opinia obejmuje min.: podstawę prawną przetwarzania danych, ocenę zgodności celu przetwarzania, tzn. czy cel instalacji kamer jest konkretny, wyraźny i zgodny z prawem, czy monitoring nie narusza zasady minimalizacji – tzn. czy kamery obejmują tylko niezbędne obszary, czy zapewniono transparentność i obowiązek informacyjny - tzn. czy zapewnione zostaną właściwe informacje dla osób, których dane dotyczą np. tabliczki informacyjne, klauzule informacyjne, czy spełniony zostanie obowiązek z art. 13 RODO.)

podpis IOD

Wniosek akceptuję. Wyrażam zgodę na:

podpis Kanclerza

* właściwe podkreślić

.....
miejscowość, data

**Dział Bezpieczeństwa
Politechniki Poznańskiej**

.....
nr wniosku

.....
miejscowość data wpływu

WNIOSEK

o zabezpieczenie/udostępnienie * nagrań z monitoringu wizyjnego

I. DANE OSOBY WNIOSKUJĄCEJ

.....
Imię Nazwisko

.....
adres

.....
nr telefonu

.....
Nazwa instytucji wnoszącego o udostępnienie nagrań

II. DATA, GODZINA, DOKŁADNE MIEJSCE ZDARZENIA

III. KRÓTKI OPIS ZDARZENIA

IV. UZASADNIENIE WNIOSKU, WSKAZANIE PODSTAWY PRAWNEJ

.....
czytelny podpis wnioskodawcy

Wyrażam zgodę / nie wyrażam zgody*

.....
czytelny podpis osoby odpowiedzialnej za udostępnienie nagrań

Potwierdzam odbiór nagrań i oświadczam, że otrzymane materiały zostaną wykorzystane wyłącznie w celu wskazanym we wniosku.

.....
data, czytelny podpis wnioskodawcy

* właściwe podkreślić / niewłaściwe skreślić

|

KLAUZULA INFORMACYJNA

- dotycząca osób realizujących wnioski o udostępnienie/zabezpieczenie nagrań z monitoringu

Na podstawie art. 13 ust. 1 i 2 Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) – (zwanym w dalszej części „RODO”) informujemy, że:

- 1) Administratorem Państwa danych osobowych jest Politechnika Poznańska zwana dalej Uczelnią, ul. Jacka Rychlewskiego 1, 61 – 131 Poznań, tel. 61 665 3639, NIP: 777 – 00 – 03 - 699, REGON: 000001608,
- 2) W sprawach związanych z ochroną danych osobowych można skontaktować się z Inspektorem Ochrony Danych, pisząc na adres e-mail: iod@put.poznan.pl lub telefonicznie pod numerem telefonu: 61 665 3631.
- 3) Państwa dane osobowe przetwarzane będą:
 - a) w celu realizacji złożonego wniosku – w związku z art. 18 RODO,
 - b) w celu wypełnienia obowiązków prawnych ciążących na administratorze w szczególności związanych z archiwizacją dokumentacji - zgodnie z art. 6. ust. 1 lit. c RODO w związku z Ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2020 r. poz. 164).
- 4) Okres przetwarzania Państwa danych osobowych jest uzależniony od celu w jakim dane są przetwarzane. Okres przechowywania wynikać będzie z przepisów prawa dotyczących archiwizacji, instrukcji kancelaryjnej i archiwalnej na podstawie Jednolitego Rzeczowego Wykazu Akt obowiązującego w Uczelni.
- 5) Mogą Państwo żądać od Administratora dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania.
- 6) Mają Państwo prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uznają, że przetwarzanie Państwa danych osobowych narusza przepisy RODO.
- 7) Podanie danych osobowych jest warunkiem realizacji wniosku. Odmowa podania danych osobowych uniemożliwia jego realizację.
- 8) W oparciu o udostępnione dane osobowe Administrator nie będzie podejmował wobec Państwa zautomatyzowanych decyzji, w tym decyzji będących wynikiem profilowania.

ARKUSZ AKTUALIZACYJNY

