Biuro Bezpieczeństwa Informacji **Urzędu Miasta Lublin** **Oznaczenie sprawdzenia: 5/2020**	Lublin, dnia 9 kwietnia 2020 r.

Sprawozdanie ze sprawdzenia w Szkole Podstawowej nr 16 im. Fryderyka Chopina w Lublinie

Spis treści

I. Informacje ogólne dotyczące przeprowadzonego sprawdzenia.

Przedmiot sprawdzenia	Weryfikacja: 1) przestrzegania ogólnych zasad przetwarzania danych osobowych w tym minimalnych wymagań w zakresie bezpieczeństwa informacji; 2) funkcjonowania systemu monitoringu wizyjnego na terenie jednostki; 3) procesu rekrutacji w zakresie spełnienia wymogów ochrony danych osobowych; 4) przestrzegania minimalnych wymogów zabezpieczeń systemów teleinformatycznych.
Oznaczenie Administratora i jego siedziby	Szkoła Podstawowa nr 16 im. Fryderyka Chopina, ul. Poturzyńska 2, 20-853 Lublin.
Termin sprawdzenia	26 lutego - 4 marca 2020 r.
Imię i nazwisko Inspektora Ochrony Danych	Witold Przeszlakowski
Imiona, nazwiska osób biorących udział w sprawdzeniu	Katarzyna Skowyra, Aleksander Czubacki Nadzorujący: Grzegorz Tymecki, Tomasz Pałysewicz

II. Ocena zgodności przetwarzania danych chronionych z przepisami prawa powszechnie obowiązującego, aktami prawa wewnętrznego oraz politykami.

Oceny dokonano na podstawie kryteriów określonych przez Biuro Bezpieczeństwa Informacji w oparciu o obowiązujące w tym zakresie przepisy prawa oraz regulacje wewnętrzne.

Stwierdzono, że Dyrektor Szkoły:

1. **z 6 kryteriów zgodności przestrzegania minimalnych wymagań bezpieczeństwa informacji wynikających z SZBI:**

a. **spełnił 4 kryteria:**

- Dokumentacja wchodząca w skład systemu Zarządzania Bezpieczeństwem Informacji została dostosowana do zaktualizowanych 30 kwietnia 2019 r. Minimalnych Wymogów Systemu Zarządzania Bezpieczeństwem Informacji. Wyznaczono IOD oraz zgłoszono go do UODO, a także wyznaczono osobę pełniącą funkcję ASI w jednostce.
- Pracownicy, stażyści i praktykanci zostali zapoznani z PBI i RBI oraz złożyli stosowne oświadczenia w tym zakresie.
- Pracownicy, stażyści i praktykanci posiadali upoważnienia do przetwarzania danych osobowych w zakresie wykonywanych przez nich obowiązków (w tym pracownicy realizujący proces rekrutacji oraz mający dostęp do monitoringu wizyjnego).
- Archiwum spełnia podstawowe wymogi wynikające z Instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego lub składnicy akt Jednostek oświatowych miasta Lublin.

b. **spełnił częściowo 2 kryteria:**

- Nie wszystkie osoby zaangażowane w proces rekrutacji pracowników oraz posiadające dostęp do monitoringu wizyjnego zostały wymienione w RCP. Ponadto wskazano nieprawidłowy okres przechowywania nagrań z monitoringu wizyjnego. RCP nie został zaktualizowany o porozumienie dotyczące przetwarzania danych. Analiza ryzyka nie była prowadzona na bieżąco.

- Stwierdzono 1 przypadek nieprawidłowego ustawienia monitora komputera na którym przetwarzane są dane osobowe.

2. **z 8 kryteriów zgodności funkcjonowania systemu monitoringu wizyjnego na terenie jednostki** wynikających z Prawa oświatowego oraz Kodeksu Pracy:

a. **spełnił 7 kryteriów;**
- W regulaminie pracy ustalono cel, zakres i sposób zastosowania monitoringu wizyjnego.
- Przeprowadzono uzgodnienie stosowania monitoringu wizyjnego z organem prowadzącym oraz wszystkie konsultacje wymagane ustawą Prawo Oświatowe.
- Uczniowie oraz pracownicy szkoły są informowani o stosowaniu monitoringu wizyjnego w jednostce.
- Pracownicy zatrudnieni po 1 stycznia 2019 r. posiadają w swoich aktach osobowych informacje o celu, zakresie i sposobie zastosowania monitoringu.
- Monitoring w szkole obejmuje swoim zasięgiem basen oraz stołówkę szkolną. Spełniono przesłanki monitorowania tych pomieszczeń.
- Klauzule informacyjne dotyczące monitoringu wywieszone są w miejscach ogólnodostępnych, a pomieszczenia i teren monitorowany są prawidłowo oznaczone.
- Nagrania z monitoringu przechowywane są przez okres krótszy niż 3 miesiące.

b. **spełnił częściowo 1 kryterium:**
- Stosowanie monitoringu w jednostce jest niezbędne i adekwatne do zapewnienia bezpieczeństwa uczniom i pracownikom jednostki oraz ochrony mienia. Brak jest natomiast dokumentacji potwierdzającej zasadność stosowania monitoringu w szkole.

3. **z 3 kryteriów zgodności procesu rekrutacji** w zakresie ochrony danych osobowych:

a. **spełnił 1 kryterium:**
- Dokumentacja związana z procesami rekrutacyjnymi jest archiwizowana zgodnie z właściwą kategorią archiwalną wynikającą z JRWA

b. **spełnił częściowo 1 kryterium**
- obowiązek informacyjny nie jest realizowany wobec wszystkich osób, których dane są przetwarzane w procesach rekrutacyjnych. Obowiązek informacyjny nie był spełniony wobec osób składających podanie do pracy poza ogłoszoną rekrutacją oraz wobec stażystów. Pozostałe klauzule informacyjne są kompletne i dostosowane do konkretnej kategorii osób, których dane osobowe są przetwarzane.

c. **nie wypełnił 1 kryterium**:
- w procesach rekrutacyjnych występują przypadki nadmiarowego przetwarzania danych osobowych.

4. **z 8 kryteriów zgodności wymogów zabezpieczeń systemu teleinformatycznego:**

a. **spełnił 1 kryterium:**
- nie instalowano oprogramowania wymagającego licencji niezgodnie z jej postanowieniami, na większości jednostek roboczych nie przechowywano plików multimedialnych, które nie są związane z wykonywaniem obowiązków służbowych.

b. **spełnił częściowo 4 kryteria:**
- częściowo stosowano zabezpieczenia danych chronionych zapewniające poufność oraz przeciwdziałające dostępowi osób nieupoważnionych,
- na stacjach roboczych objętych sprawdzeniem częściowo stosowano zabezpieczenia wymagane w RSI,
- część z kluczowych elementów systemu teleinformatycznego posiada zasilanie awaryjne,
- pomieszczenie serwerowni częściowo spełnia wymagania określone w RSI.

c. **nie wypełnił 3 kryteriów:**
- nie zapewniono rozliczalności użytkowników w systemach poczty elektronicznej i monitoringu,
- nie zastosowano właściwych poziomów dostępu dla użytkowników systemu teleinformatycznego, nie zdeponowano wszystkich haseł administracyjnych do systemów teleinformatycznych,
- nie zapewniono zdolności do szybkiego przywrócenia dostępności danych w razie incydentu.

Ustalenia ze sprawdzenia opisano w nw. arkuszach, sporządzonych na podstawie szczegółowych list kontrolnych, które stanowią dokumentację niniejszego sprawdzenia.

III. Arkusze szczegółowe

a) Funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji w Jednostce

Kryterium nr 1 **aktualizacja dokumentacji, wyznaczenie i zgłoszenie IOD, wyznaczenie ASI**	**Aktualizacja dokumentacji SZBI obowiązującej w JOM oraz spełnienie wymogu wyznaczenia i zgłoszenia IOD do UODO oraz wyznaczenie ASI.** Kryterium oceny: W przypadku gdy spośród następujących warunków: -jednostka posiada aktualną dokumentację SZBI -wyznaczony został IOD – fakt ten został zgłoszony do UODO oraz wyznaczony został ASI. Jednocześnie zostały zrealizowane oba warunki – **kryterium spełnione** został zrealizowany 1 z nich – **kryterium spełnione częściowo** nie zostały zrealizowane obydwa – **kryterium niespełnione**

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
1. Na podstawie Zarządzenia Dyrektora nr 94/2019 z dnia 20 maja 2019 r. w jednostce wdrożono Politykę Bezpieczeństwa Informacji, Regulamin Bezpieczeństwa Informacji oraz Regulamin Systemu Informatycznego. Ww. dokumentacja została zaktualizowana do Minimalnych Wymogów Systemu Zarządzania Bezpieczeństwem Informacji wprowadzonych pismem Prezydenta z dnia 30.04.2019 r. 2. IOD został wyznaczony Zarządzeniem Dyrektora nr 54a/2018 z dnia 23.07.2018 r. IOD został zgłoszony do UODO w dniu 8 sierpnia 2018 r. 3. W dniu 21 stycznia 2020 r. powołano Administratora Systemu Informatycznego (Marcin Zmysłowski). Z wyjaśnień dyrektora wynika, iż obowiązki ASI w jednostce pełnił również informatyk szkoły (Marek Gielara). Ww. osoba nie została formalnie powołana do pełnienia roli ASI. Dyrektor szkoły, zarządzeniem nr 123/2020 z dnia 06.03.2020 r. powołał Pana Marka Gielarę na stanowisko ASI (wg. informacji przekazanej do BI w dniu 06.04.2020 r.).	Kryterium spełnione	Panu Markowi Gielera należy powierzyć pełnienie funkcji ASI w jednostce w sposób formalny. **Termin realizacji: Zrealizowane** **Osoba odpowiedzialna: Dyrektor**

Kryterium nr 2 **aktualizacja rejestrów oraz analizy ryzyka**	**Bieżące prowadzenie: RCP, RUP, RKP oraz AR w kontekście zagadnień objętych przedmiotem sprawdzenia (monitoring wizyjny, rekrutacja pracowników).** Kryterium oceny: -zaktualizowano RCP, RKP, RUP i AR – **kryterium spełnione** -nie zaktualizowano 2 z ww. rejestrów lub AR – **kryterium spełnione w części** -nie zaktualizowano RCP, RKP, RUP i AR – **kryterium niespełnione**

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
RUP został zaktualizowany o umowę powierzenia tj. Porozumienie nr 117/IT/19 zawarte z Wydziałem IT UM Lublin z dnia 21 marca 2019 r. dotyczącej przetwarzania danych osobowych. **RCP** nie był prowadzony w sposób rzetelny i bieżący ponieważ: -nie uwzględniono w nim wszystkich osób, które mają dostęp do systemu monitoringu a także biorących udział w rekrutacji pracowników; - nie zaktualizowano RCP w zakresie ww. porozumienia nr 117/IT/19; -wskazano nieprawidłowy czas przetwarzania nagrań z monitoringu wizyjnego;	Kryterium spełnione w części	1.Wskazać w RCP wszystkie osoby zaangażowane w proces rekrutacji pracowników oraz mające dostęp do monitoringu wizyjnego w jednostce. 2. Uzupełnić RCP o podmiot przetwarzający (porozumienie z Wydziałem IT UM Lublin) 3.Wskazać w RCP rzeczywisty czas przetwarzania nagrań z monitoringu wizyjnego.

Wg. **AR,** wartość ryzyka dla poszczególnych ryzyk związanych z funkcjonowaniem systemu monitoringu wizyjnego oceniono na; poufność - 22, integralność - 12 dostępność - 18. W ww. dokumencie, jako przyczynę utraty dostępności do danych z systemu monitoringu wpisano cyt. kradzież dokumentacji papierowej. Dane z systemu monitoringu przetwarzane są jedynie w wersji elektronicznej. Ponadto jako właściciela ryzyka we wszystkich 3 atrybutach wskazano inspektora BHP, który faktycznie nie ma dostępu do tego aktywa. W **AR**, wartość ryzyka dla poszczególnych ryzyk związanych z procesem rekrutacji pracowników oceniono na: poufność - 28, integralność - 28 dostępność – 28. W ww. dokumencie nie uwzględniono specjalisty ds. administracyjnych jako właściciela ryzyka, pomimo tego, że odbierając korespondencję od kandydatów do pracy, przetwarza ich dane osobowe.		4.Aktualizować na bieżąco analizę ryzyka w szczególności wskazać osoby, które rzeczywiście przetwarzają dane za pomocą systemu monitoringu. **Termin realizacji: 30.04.2020r** **Osoba odpowiedzialna:** **Punkt 1, 3, 4 – Jarosław Kasperek (kierownik gospodarczy)** **Punkt nr 2 – Marcin Zmysłowski (ASI)**

Kryterium nr 3 **wiedza pracowników nt. SZBI**	**Pracownicy/stażyści złożyli oświadczenie o zapoznaniu się i zobowiązaniu do stosowania zapisów PBI oraz RBI zawierające wszystkie elementy określone w załączniku nr 1 do RBI (w tym oświadczenie o zachowaniu w tajemnicy informacji chronionej).** Kryterium oceny: -więcej niż 90% badanych przypadków – **kryterium spełnione** -80-90% badanych przypadków – **kryterium spełnione w części** -poniżej 80% badanych przypadków – **kryterium niespełnione**		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
Na podstawie weryfikacji dokumentacji: - 31 z 141 pracowników szkoły; -wszystkich 3 stażystów odbywających staż w szkole od 25 maja 2018 r.; -10 z 18 praktykantów odbywających praktyki w szkole w roku 2019/2020 stwierdzono, że wszystkie ww. osoby podpisały oświadczenie o zapoznaniu się z PBI oraz RBI (oświadczenia zawierają informację o zobowiązaniu do zachowania w tajemnicy informacji chronionych Jednostki). Oświadczenia, są zgodne z wzorem będącym załącznikiem do Polityki Bezpieczeństwa Informacji.		Kryterium spełnione	Nie dotyczy

Kryterium nr 4 **upoważnienia i oświadczenia w zakresie danych osobowych**	**Pracownicy/stażyści posiadają upoważnienia do przetwarzania danych osobowych w zakresie wykonywanych przez nich obowiązków (w tym pracownicy realizujący proces rekrutacji, monitoringu wizyjnego).** Kryterium oceny: -więcej niż 90% badanych przypadków – **kryterium spełnione** -80-90% badanych przypadków – **kryterium spełnione w części** -poniżej 80% badanych przypadków – **kryterium niespełnione**		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
W szkole prowadzona była ewidencja osób upoważnionych, która byłą zgodna ze wzorem z załącznika nr 5 do PBI. Ewidencja prowadzona była na bieżąco. W ewidencji uwzględniono m.in. daty wstrzymania upoważnień. Brak nadanych pracownikom identyfikatorów w systemie informatycznym. We wszystkich spośród 31 poddanych próbie akt osobowych, znajdowały się ww. upoważnienia. Wszystkie osoby mające dostęp do systemu monitoringu wizyjnego oraz do danych osobowych pozyskiwanych w procesie rekrutacji zostały upoważnione, w stosownym zakresie.		Kryterium spełnione	Uzupełnić ewidencję upoważnień o identyfikatory w systemie informatycznym. **Termin realizacji: Zrealizowane** **Osoba odpowiedzialna: Anna Pieczykolan (spec.ds.**

Od 25 maja 2018, 3 osoby odbywały staż w szkole. Wszystkie z nich otrzymały upoważnienia do przetwarzania danych osobowych na czas odbywania stażu. Na podstawie próby 10 z 18 osób odbywających praktyki w roku szkolnym 2019/2020 stwierdzono, że wszystkie ww. osoby otrzymały upoważnienia do przetwarzania danych osobowych. Upoważnienia pracowników, stażystów i praktykantów prowadzone były na wzorze określonym w PBI. Dnia 06.04.2020 r. okazano uzupełnioną ewidencję upoważnień o identyfikatory w systemie informatycznym.		**administracyjnych)**

Kryterium nr 5 **zabezpieczenia fizyczne pomieszczeń**	**Stosowanie zabezpieczeń fizycznych zapewniających poufność, integralność oraz dostępność danych** Sposoby ochrony danych przechowywanych/przetwarzanych przez jednostkę: -zabezpieczenia dokumentacji papierowej (zamykane na klucz pomieszczenia, szafy, szuflady), -stanowiska na których przetwarzane są dane podlegające ochronie uniemożliwiają osobom postronnym dostęp do danych (zasada czystego biurka i czystego ekranu, prawidłowe ustawienie monitora), -dokumenty przeznaczone do zniszczenia niszczone są w sposób uniemożliwiający identyfikację zawartych na nich danych, -karty kryptograficzne zabezpieczane są przed dostępem osób nieuprawnionych. Kryterium oceny: W przypadku gdy spełnione są wszystkie z ww. warunków w: -więcej niż 90 % badanych przypadków – **kryterium spełnione** -80-90 % badanych przypadków – **kryterium spełnione w części** -poniżej 80 % badanych przypadków – **kryterium niespełnione**

Ustalenia	**Ocena zgodności**	**Termin realizacji, wskazanie osoby odpowiedzialnej za realizację oraz uwagi**
Na podstawie przeprowadzonych oględzin 7 pomieszczeń ustalono, że: 1. Wszystkie weryfikowane pomieszczenia były zamykane na klucz (pokoje wicedyrektorów, sekretariat, pokój pedagogów i doradcy zawodowego, pokój kierownika gospodarczego, kierownika obiektów sportowych i inspektora bhp, pokój kadrowej, sala z rejestratorami monitoringu wizyjnego). Klucze do ww. pomieszczeń są zabierane przez pracowników do domu z uwagi na brak portierni. 2. Na 1 z 7 (14%) weryfikowanych pomieszczeń stwierdzono stanowisko pracy, na którym monitor komputera ustawiony był w sposób umożliwiający wgląd osobie postronnej w jego zawartość. (komputer kierownika obiektów sportowych), 3. We wszystkich weryfikowanych pomieszczeniach, dokumenty zawierające dane osobowe są odpowiednio zabezpieczane w szafach i regałach zamykanych na klucz. 4. We wszystkich weryfikowanych pomieszczeniach, w których przetwarza się dane osobowe w formie papierowej znajdują się niszczarki. 5. Karty kryptograficzne wszystkich weryfikowanych pracowników były odpowiednio zabezpieczone przed dostępem osób nieupoważnionych.	Kryterium spełnione w części	Ustawić monitor komputera kierownika obiektów sportowych w sposób uniemożliwiający wgląd w jego zawartość osobom postronnym. **Termin realizacji: 30.04.2020r** **Osoba odpowiedzialna: Jarosław Kasperek (kierownik gospodarczy)**

Kryterium nr 6 **zabezpieczenia fizyczne archiwum**	**Zabezpieczenia danych osobowych w pomieszczeniu archiwum** powinny spełniać minimalne wymagania wymienione poniżej: -drzwi antywłamaniowe i przeciwpożarowe, -czujnik temperatury, -czujnik wilgotności, -czujnik dymu wraz z możliwością alarmowania, -sprawna gaśnica w pomieszczeniu, -ograniczenie dostępu do pomieszczenia tylko dla upoważnionych przez Kierownika Jednostki pracowników, -regały metalowe lub drewniane przeznaczone na przechowywanie dokumentacji z pierwszą półką na wysokości min. 15 cm, Kryterium oceny: W przypadku gdy pomieszczenie archiwum spełnia: co najmniej 5 ww. warunków – **kryterium spełnione** 3 do 4 ww. warunków – **kryterium częściowo spełnione** mniej niż 3 ww. warunki – **kryterium niespełnione** **W przypadku gdy w pomieszczeniu archiwum brak jest czujnika dymu wraz z możliwością alarmowania niezależnie od ilości spełnionych warunków kryterium zostanie uznane za niespełnione**

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
Pomieszczenie archiwum usytuowane jest na parterze budynku. Drzwi wejściowe są antywłamaniowe i przeciwpożarowe, plombowane po każdym wyjściu. W pomieszczeniu znajduje się czujnik dymu oraz termohigrometr wg. którego archiwista na bieżąco prowadzi rejestr parametrów środowiska. Archiwum wyposażone jest w gaśnice, koc gaśniczy i worki ewakuacyjne. W oknach zamontowano wertykale i kraty. Dokumentacja umieszczona jest na metalowych i drewnianych regałach z pierwszą półką powyżej 15 cm. Dostęp do archiwum możliwy jest jedynie w obecności archiwisty.	Kryterium spełnione	Nie dotyczy

b) Monitoring wizyjny

Kryterium nr 1 **spełnienie przesłanek funkcjonowania monitoringu**	**Niezbędność i adekwatność stosowania w Szkole monitoringu.** **Występowanie przesłanek stosowania w Szkole monitoringu wizyjnego (zapewnienie bezpieczeństwa uczniów i pracowników, ochrona mienia) np. udokumentowane akty wandalizmu, uszkodzenia/ kradzieży mienia, bójek, itp.** Kryteria oceny: **Kryterium spełnione**- występują udokumentowane przesłanki stosowania monitoringu zgodnie z art .108a ust. 1 Prawa Oświatowego **Kryterium spełnione w części** – nie udokumentowano występowania ww. przesłanek **Kryterium niespełnione**- nie występują przesłanki stosowania monitoringu określone w art .108a ust. 1 Prawa Oświatowego

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
Z wniosku o uzgodnienie z organem prowadzącym stosowania monitoringu wynika, iż cyt.: "celem stosowania monitoringu jest konieczność zapewnienia bezpieczeństwa uczniów i pracowników oraz ochrona mienia. Powyższe uzasadnione jest bezpieczeństwem dzieci i młodzieży przebywających na terenie szkoły. Zainstalowanie kamer ma także pełnić funkcje prewencyjne, w celu zabezpieczenia uczniów przed kradzieżami i wandalizmem, które mogą się zdarzyć". Wg. wyjaśnień Dyrektora, w szkole występowały kradzieże rowerów oraz bójki między uczniami. W szkole nie dokumentowano faktu występowania ww. zdarzeń.	Kryterium spełnione w części	Prowadzić dokumentację związaną z występującymi w Szkole przypadkami aktów wandalizmu, uszkodzeniami/kradzieżami mienia oraz zdarzeniami zagrażającymi bezpieczeństwu uczniów i pracowników (np. notatki służbowe, zgłoszenia na policje). **Termin realizacji: Dokumentacja będzie prowadzono na bieżąco.** **Osoba odpowiedzialna:** Jarosław Kasperek (kierownik gospodarczy)

Kryterium nr 2 **dostosowanie regulaminu pracy**	**Ustalenie w regulaminie pracy jednostki celu, zakresu oraz sposobu zastosowania monitoringu,** zgodnie z art 22^2 §6 Kodeksu Pracy Kryteria oceny: **Kryterium spełnione**- cel, zakres i sposób zastosowania wpisano w regulaminie pracy. **Kryterium niespełnione**- nie określono w regulaminie celu, zakresu i sposobu zastosowania monitoringu.

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
W Regulaminie Pracy (Aneks wprowadzony Zarządzeniem Dyrektora nr 93/2019 z dnia 25 marca 2019 r.) ustalono: **Cel stosowania** - "W celu zapewnienia bezpieczeństwa pracowników oraz ochrony mienia, oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę w budynkach szkoły oraz na terenie wokół budynków szkoły stosuje się nadzór w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring wizyjny)"; **Zakres monitoringu** - "a) budynek zaplecza socjalno-szatniowego; b) budynek główny "A", budynek sportowy "B"; c) budynek niski "C' oraz teren wokół szkoły; Monitoring swoim zasięgiem nie obejmuje szatni pracowniczej, klasopracowni, pomieszczeń administracyjnych, pomieszczeń świetlicy szkolnej, oraz holu głównego na II piętrze". **Sposób zastosowania** - "monitoring wizyjny jest prowadzony w sposób ciągły przez 24 godziny na dobę i odbywa się poprzez bieżący zapis obrazu kamer przemysłowych obejmujących monitorowane obszary".	Kryterium spełnione	Nie dotyczy

Kryterium nr 3 przeprowadzenie uzgodnień i konsultacji	**Uzgodnienie stosowania monitoringu z organem prowadzącym, przeprowadzenie konsultacji z radą pedagogiczną, radą rodziców oraz z samorządem uczniowskim. Fakt uzgodnienia i konsultacji został udokumentowany.** Kryteria oceny: **Kryterium spełnione** - przeprowadzono wszystkie uzgodnienia i konsultacje. **Kryterium spełnione częściowo** - monitoring uzgodniono z co najmniej z dwoma organami jednostki. **Kryterium niespełnione** - nie przeprowadzono żadnych uzgodnień.		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
Monitoring w Szkole został uzgodniony z **organem prowadzącym** 12 lutego 2020 r. Konsultacje z **radą pedagogiczną** przeprowadzono w dniu 25 czerwca 2019 r. co udokumentowano Uchwałą nr 215/2018/2019 dot. pozytywnego zaopiniowania regulaminu monitoringu wizyjnego. Konsultacje z **radą rodziców** przeprowadzono w dniu 13 czerwca 2019 r. co udokumentowano Uchwałą nr 16/2018/2019 dot. pozytywnego zaopiniowania regulaminu monitoringu wizyjnego. Konsultacje z **samorządem uczniowskim** przeprowadzono w dniu 13 czerwca 2019 r. co udokumentowano Uchwałą nr 3/2018/2019 dot. pozytywnego zaopiniowania regulaminu monitoringu wizyjnego.		Kryterium spełnione	Nie dotyczy

Kryterium nr 4 informacja społeczności szkolnej o monitoringu	**Spełnienie przez Dyrektora jednostki obowiązku poinformowania uczniów i pracowników szkoły o wprowadzeniu monitoringu. Fakt poinformowania został udokumentowany.** Kryteria oceny: **Kryterium spełnione** - poinformowanie uczniów i pracowników **Kryterium spełnione częściowo**- przekazano informację przynajmniej jednej kategorii podmiotów **Kryterium niespełnione**- nie przekazano informacji żadnym podmiotom		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
Wg wyjaśnień Dyrektora, uczniowie są informowani o stosowaniu monitoringu na pierwszych spotkaniach z wychowawcą oraz na apelu rozpoczynającym rok szkolny. We wszystkich poddanych próbie aktach osobowych pracowników widniały klauzule informacyjne dotyczące stosowania monitoringu wizyjnego w szkole.		Kryterium spełnione	Nie dotyczy

Kryterium nr 5 informowanie nowych pracowników o monitoringu	**Spełnienie przez Dyrektora jednostki obowiązku informowania na piśmie o stosowanym monitoringu osób zatrudnionych po 1 stycznia 2019 r. przed dopuszczeniem ich do wykonywania obowiązków służbowych (art. 108a ust. 7 Prawa Oświatowego oraz §3 ust f Rozporządzenia w sprawie dokumentacji pracowniczej)** Kryteria oceny: **Kryterium spełnione** - przekazanie ww. informacji przed dopuszczeniem nowego pracownika do pracy. **Kryterium spełnione częściowo** - przekazanie ww. informacji do 1 miesiąca od rozpoczęcia pracy. **Kryterium niespełnione** - nie przekazano ww. informacji.		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
Po 1 stycznia 2019 r. w szkole zatrudniono 32 pracowników. W wyniku weryfikacji 12 z 32 akt osobowych ww. pracowników stwierdzono, że we wszystkich aktach znajdują się potwierdzenia poinformowania pracowników o celu, zakresie i sposobie zastosowania monitoringu.		Kryterium spełnione	Nie dotyczy

Kryterium nr 6 rozmieszczenie kamer	**Rozmieszczenie kamer w szkole oraz analiza ich legalności.** Kryteria oceny: **Kryterium spełnione** - monitoring wizyjny nie obejmuje pomieszczeń określonych w art. 108a ust 3 Prawa Oświatowego lub obejmuje określone w ust. 3 pomieszczenia i jednocześnie spełniono przesłanki ich monitorowania (niezbędność realizacji celu i nie naruszanie godności osób oraz zastosowano techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób). **Kryterium spełnione częściowo** - monitoring wizyjny nie obejmuje pomieszczeń określonych w art. 108a ust 3 Prawa Oświatowego lub obejmuje określone w ust. 3 pomieszczenia i jednocześnie spełniono przesłanki ich monitorowania (niezbędność realizacji celu i nie naruszanie godności osób jednak nie zastosowano technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób). **Kryterium niespełnione**- nie wypełniono wymogów określonych w art 108 a ust. 3 Prawa Oświatowego.		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
W skład systemu monitoringu wchodzą 74 kamery: Kamery zewnętrzne (26) obejmują swoim zasięgiem teren wokół szkoły, boiska oraz parkingi szkolne. Nie stwierdzono aby zasięg kamer obejmował teren niezarządzany przez jednostkę. Kamery wewnętrzne (48) obejmują swoim zasięgiem korytarze szkolne, klatki schodowe, basen i stołówkę szkolną. Na basenie znajdują się 2 kamery obejmujące swoim zasięgiem nieckę basenu. W godzinach lekcyjnych odbywają się tam zajęcia dla uczniów, natomiast po zakończeniu zajęć lekcyjnych obiekt jest wynajmowany firmom zewnętrznym na nauki pływania, fitness lub pływanie rekreacyjne. Kamery zamontowane na basenie są wyłączane na czas zajęć dydaktycznych. Monitoring uruchamiany jest na czas najmu basenu. Kamera w stołówce obejmuje swoim zasięgiem pomieszczenie przeznaczone wyłącznie dla uczniów.		Kryterium spełnione	Nie dotyczy

Kryterium nr 7 **oznaczenie monitorowanych pomieszczeń**	**Spełnienie obowiązków oznaczenia pomieszczeń i terenu monitorowanego w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych.** Kryteria oceny: **Kryterium spełnione** – klauzula informacyjna dot. monitoringu dostępna jest w miejscu ogólnodostępnym umożliwiającym zapoznanie się nią osobom przebywającym na terenie jednostki. Pomieszczenia oznakowane są piktogramami, a wejścia na teren jednostki oznakowane są informacją (skróconą lub pełną) o monitoringu. **Kryterium spełnione częściowo** – teren i budynek jednostki oznaczone są informacją o stosowaniu monitoringu (bez klauzuli informacyjnej z którą mogą zapoznać się osoby przebywające w jednostce). **Kryterium niespełnione** – brak oznaczeń pomieszczeń i terenu monitorowanego, brak pełnej klauzuli informacyjnej.

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
Przy bramie wjazdowej na parking szkolny, oraz przy 4 furtkach zamontowane zostały tabliczki o treści "obiekt monitorowany" wraz z piktogramem kamery. Na 6 drzwiach wejściowych widniały takie same tabliczki. Na korytarzach każdego segmentu szkoły, również znajdują się naklejki informujące o obiekcie monitorowanym wraz piktogramem kamery. Klauzule informacyjne znajdują się na 3 drzwiach wejściowych do szkoły (drzwi główne, wejście na basen, wejście na boisko). Osoba przebywająca na zewnątrz budynku może zapoznać się z treścią klauzuli. W 3 miejscach wewnątrz szkoły, również wywieszono klauzule informacyjne (tablice informacyjne na korytarzach). Ww. klauzule zawierają wszystkie informacje wymagane w art 13 RODO.	Kryterium spełnione	Nie dotyczy

Kryterium nr 8 **okres przetwarzania danych z monitoringu**	**Weryfikacja przestrzegania zasad dot. okresu przechowywania nagrań z monitoringu wizyjnego** Kryteria oceny: **Kryterium spełnione**: dane przechowywane są maksymalnie do 3 miesięcy (nie wliczając nagrań zabezpieczonych na wniosek organów ścigania na potrzeby postępowania dowodowego). **Kryterium niespełnione**: dane przechowywane są powyżej 3 miesięcy

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
Według RCP czas przetwarzania wynosi "do 21 dni od dnia rejestracji nagrania w zależności od ilości nagrywanych zdarzeń" . W wyniku weryfikacji w dn. 02.03.2020 r. okresu przechowywania nagrań na 6 rejestratorach stwierdzono, iż nagrania przechowywano od 19 do 101 dni. Prawidłowy okres przechowywania nagrań na rejestratorze M2 (tj. do 3 miesięcy) skorygowano niezwłocznie w toku sprawdzenia. Nagrania starsze niż 3 miesiące zostały skasowane.	Kryterium spełnione	Nie dotyczy

Kryterium nr 9 podmiot zewnętrzny obsługujący monitoring	**Obsługa monitoringu przez podmiot zewnętrzny (w tym umowa serwisowa), zawarcie umów powierzenia w tym zakresie, monitorowanie na bieżąco obrazu z kamer.** Kryteria oceny: **Kryterium spełnione** - została zawarta umowa powierzenia zgodna z art. 28 RODO z firmą obsługującą monitoring. **Kryterium spełnione częściowo** – zawarta umowa powierzenia nie spełnia wszystkich wymogów określonych w art. 28 RODO. **Kryterium niespełnione**- brak umowy powierzenia z firmą obsługującą monitoring, pomimo że posiada dostęp do danych zgromadzonych w systemie.

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
Monitoring w jednostce nie jest obsługiwany przez podmiot zewnętrzny.	Nie dotyczy	Nie dotyczy

Ustalenia dodatkowe sposób postępowania w przypadku udostępniania nagrań	**Procedura udostępniania nagrań z monitoringu.** Kryteria oceny: nie dotyczy

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
W szkole wprowadzono regulamin funkcjonowania monitoringu wizyjnego (Zarządzenie nr 98/2019 z dnia 25 czerwca 2019 r.), w którym uregulowano sposób udostępniania nagrań na zewnątrz. Zgodnie z wyjaśnieniami Dyrektora, nagrania nie były udostępniane. <u>W ww. regulaminie stwierdzono następujące nieprawidłowości:</u> -W ust. 2 wskazano nieprawidłową podstawę prawną funkcjonowania monitoringu na terenie szkoły (art. 6 ust 1 lit f – prawnie uzasadniony interes administratora). Podstawą prawną stosowania monitoringu jest art. 6 ust.1 lit. c RODO w związku z art.108a ust.1 Ustawy Prawo oświatowe oraz art. 22 Kodeksu Pracy (niezbędność wypełnienia obowiązku prawnego spoczywającego na Administratorze tj. zapewnienie bezpieczeństwa). -Zgodnie z ust. 5 regulaminu, zasięg kamer obejmuje m.in pomieszczenia takie jak: czytelnia, szatnie na ubrania zewnętrzne, umywalnie rąk. Ww. pomieszczenia faktycznie nie są objęte zasięgiem kamer. -Zgodnie z ust.18 regulaminu, nagrania mogą być (...) udostępniane do wglądu m.in. upoważnionemu ustnie przez dyrektora szkoły nauczycielowi lub innemu pracownikowi szkoły. Zgodnie z rozdz. 8.4 pkt. 4 PBI, w aktach osobowych pracownika przechowuje się oryginalny egzemplarz upoważnienia do przetwarzania danych osobowych podpisany własnoręcznie przez pracownika, co jednocześnie jest potwierdzeniem, że pracownik przyjął treść upoważnienia do wiadomości. W związku z powyższym upoważnienia powinny być nadawane jedynie w formie pisemnej. - Zgodnie z ust. 21 regulaminu, okres przechowywania nagrań wynosi do 30 dni, natomiast w związku z przeprowadzonym sprawdzeniem stwierdzono, że faktyczny okres przechowywania wynosił więcej niż 30 dni (nawet do 101 dni). - Zgodnie z ust. 23 regulaminu, osoba zainteresowana zabezpieczeniem danych z monitoringu na potrzeby przyszłego postępowania może zwrócić się pisemnie do Dyrektora z prośbą o ich zabezpieczenie przed usunięciem po upływie standardowego okresu ich przechowywania. Zgodnie z art.108a ust.4 nagrania obrazu (...) przechowuje się przez okres nie dłuższy niż 3 miesiące od dnia nagrania. - Powyższe dotyczy również zapisu z ust.29 regulaminu, wg. którego nagrania zabezpiecza się przez okres 6 miesięcy.	Nie dotyczy	Dostosować zapisy regulaminu funkcjonowania monitoringu do obowiązujących przepisów prawa. **Termin realizacji: 30.04.2020r.** **Osoba odpowiedzialna: Jarosław Kasperek (kierownik gospodarczy)**

c) Proces rekrutacji pracowników

Kryterium nr 1 **legalizm oraz minimalizacja danych**	**Przestrzeganie legalności oraz zasady „minimalizacji danych", przetwarzanych w procesach rekrutacyjnych** Kryteria oceny: **Kryterium spełnione** - Przetwarzanie wszystkich kategorii danych osobowych podczas procesów rekrutacyjnych posiada odpowiednią podstawę prawną. Zakres przetwarzanych danych jest adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane. **Kryterium niespełnione** – W procesach rekrutacyjnych występują przypadki przetwarzania danych osobowych pomimo braku odpowiedniej podstawy prawnej bądź dane przetwarzane są nadmiarowo.

Ustalenia	Ocena zgodności	Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)
Od 25 maja 2018 r. w szkole organizowano 6 naborów na stanowiska administracyjne. (informatyk, spec. ds. płac, inspektor bhp, kierownik gospodarczy, spec. ds. płac, główny księgowy). Wymagana podczas ww. naborów przeprowadzonych po maju 2019 r. (informatyk, spec. ds. płac, inspektor bhp) dokumentacja wykraczała poza dozwolony w art. 22¹ kodeksu pracy zakres informacji wymaganych od osoby ubiegającej się o zatrudnienie (obowiązujący w aktualnej treści od 04.05.2019r.) ponieważ: - Przetwarzanie danych osobowych zawartych w dowodzie osobistym lub paszporcie typu nr. PESEL, numer i seria dowodu, miejsce urodzenia, kolor oczu, wzrost, wizerunek a także wymaganie kserokopii ww. dokumentów należy uznać za nadmiarowe i naruszające zasadę minimalizacji danych, o której mowa w art. 5 ust.1 lit. c RODO. Wymaganie od kandydatów do pracy ww. danych, narusza również art 22¹ par. 3 kodeksu pracy zgodnie z którym, nr PESEL, a w przypadku jego braku rodzaj i numer dokumentu potwierdzającego tożsamość, pracodawca może żądać dopiero od pracownika (tj. osoby już zatrudnionej). Wykonywanie kserokopii ww. dokumentów jest niedopuszczalne. -Dokument poświadczający referencje z poprzedniego miejsca pracy został ujęty w "wymaganych dokumentach", nie jest więc pozyskany z inicjatywy osoby ubiegającej się o zatrudnienie. - Zgodnie z Rozporządzeniem Rady Ministrów z dnia 15 maja 2018 r. w sprawie wynagradzania pracowników samorządowych, staż pracy dla kandydatów na pracowników administracyjnych w jednostkach organizacyjnych nie jest wymagany we wszystkich przypadkach. W ww. ogłoszeniach o naborze, wymagano kserokopii świadectw pracy od wszystkich kandydatów, zarówno posiadających średnie wykształcenie jak i wyższe. Po zatrudnieniu pracownika pozyskiwany jest od niego kwestionariusz osobowy - zgodny ze wzorem kwestionariusza osobowego dla pracownika zamieszczonego na stronie Ministerstwa Rodziny, Pracy i Polityki Społecznej.	Kryterium niespełnione	W procesie rekrutacji pracowników, pobierać wyłącznie dane niezbędne do wyłonienia kandydata do pracy, określonych w odpowiednich przepisach prawa (Kodeks Pracy, Karta Nauczyciela, Ustawa o pracownikach samorządowych). **Termin realizacji: Od czasu kontroli będą pozyskiwane tylko dane niezbędne** **Osoba odpowiedzialna: Liliana Kurębska (spec. ds. kadrowych)**

Kryterium nr 2 **realizacja obowiązku informacyjnego w procesie rekrutacji**	**Realizacja obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane w procesach rekrutacyjnych, zgodnie z art. 13 RODO.** Kryteria oceny: **Kryterium spełnione** – Obowiązek informacyjny jest realizowany wobec wszystkich osób, których dane osobowe są przetwarzane w procesach rekrutacyjnych. Klauzule informacyjne są kompletne i dostosowane do konkretnej kategorii osób, których dane osobowe są przetwarzane. **Kryterium spełnione częściowo** – Obowiązek informacyjny nie jest realizowany wobec wszystkich kategorii osób, których dane osobowe są przetwarzane. Wykorzystywane klauzule informacyjne są niekompletne lub niedostosowane do konkretnej kategorii osób, których dane są przetwarzane. **Kryterium niespełnione** – Brak realizacji obowiązku informacyjnego.		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
Od 25 maja 2018 r. w szkole zatrudniono 49 pracowników w tym: 1. 6 pracowników administracyjnych: Na stanowiska pracowników administracyjnych ogłaszane były publiczne nabory (ogłoszenie w BIP). Wszystkie poddane próbie akta pracowników (5 akt) zawierały klauzule informacyjne do rekrutacji, oraz dla pracowników szkoły. Z wyjaśnień specjalisty ds. kadr obowiązek informacyjny był również spełniany wobec nieprzyjętych kandydatów do pracy. Ww. informacji nie można zweryfikować ponieważ dokumentacja aplikacyjna ww. osób została komisyjnie zniszczona. 2. 35 pracowników pedagogicznych: Wszyscy ww. pracownicy zostali przeniesieni z innych placówek bez organizacji konkursów na stanowiska. W związku z powyższym klauzule do rekrutacji nie były im przekazywane, natomiast klauzule dla pracowników znalazły się we wszystkich poddanych próbie aktach osobowych ww. osób (7). 3. 8 pracowników obsługi: Ww. pracownicy podobnie jak w przypadku pracowników pedagogicznych, zostali przeniesieni z innych placówek, więc klauzule dla kandydatów do pracy nie były im przekazywane. Klauzule dla pracowników znalazły się w weryfikowanych aktach osobowych (1). Wobec kandydatów do pracy, którzy przesyłają swoją dokumentację aplikacyjną w czasie kiedy na dane stanowisko nie, nie jest prowadzona rekrutacja jest realizowany obowiązek informacyjny. Przesyłane CV jest usuwane a nadawca jest informowany o braku zapotrzebowania na nowych pracowników. Zgodnie z art. 13 ust 1 RODO cyt: jeżeli dane osobowe osoby, której dane dotyczą zbierane są od tej osoby, Administrator podczas pozyskiwania danych osobowych podaje jej wszystkie informacje (opisane w art. 13 ust 1 lit a-f). Stażyści odbywający staż w szkole od 25 maja 2018 r. (3) nie otrzymywali klauzul informacyjnych dla stażystów. Praktykanci odbywający praktyki w roku szkolnym 2019/2020 otrzymywali klauzule informacyjne dla praktykantów. (sprawdzono na podstawie 10 z 18 osób).	Kryterium spełnione częściowo	Zapewnić prawidłową realizację obowiązku informacyjnego wobec osób składających podanie o przyjęcie do pracy oraz stażystów. **Termin realizacji: Realizacja obowiązku informacyjnego w procesie rekrutacji jest prowadzona na bieżąco.** **Osoba odpowiedzialna: Liliana Kurębska (spec.ds. kadrowych)**

Kryterium nr 3 **okres przetwarzania danych z rekrutacji**	**Przestrzeganie zasady „ograniczenia przechowywania" danych osobowych przetwarzanych w procesach rekrutacyjnych, zgodnie z art. 5 ust. 1 lit. e RODO oraz obowiązującym JRWA** Kryteria oceny: **Kryterium spełnione** – Dokumentacja związana z procesami rekrutacyjnymi jest rejestrowana oraz archiwizowana zgodnie z właściwą kategorią archiwalną wynikającą z JRWA **Kryterium niespełnione** – Dokumentacja związana z procesami rekrutacyjnymi nie jest rejestrowana lub jest archiwizowana z naruszeniem wymogów wynikających z kategorii archiwalnej określonej na podstawie JRWA.		
Ustalenia		**Ocena zgodności**	**Wnioski i zalecenia (wraz ze wskazaniem osoby odpowiedzialnej za realizację oraz terminem realizacji)**
Z przeprowadzanych naborów na stanowiska administracyjne sporządzane są protokoły. Raz w roku zdawane są do archiwum, gdzie następnie przechowywane są przez 2 lata licząc od końca roku w którym nabór został przeprowadzony. Wg .wyjaśnień dyrektor, po wyłonieniu zwycięzcy naboru na stanowisko, dokumenty aplikacyjne osoby niezatrudnionej są protokolarnie niszczone (okazano protokoły). Dokumenty osoby, która zakończyła pracę są archiwizowane przez 10 lub 50 lat. Dokumentacja kandydatów do pracy przesłana drogą elektroniczną, w przypadku gdy nie jest prowadzony nabór lub konkurs, nie jest rejestrowana ani klasyfikowana według kategorii z JRWA.		Kryterium spełnione	**Sposób postępowania z dokumentacją rekrutacyjną**: W przypadku naboru na pracownika samorządowego, dokumenty aplikacyjne osoby zatrudnionej należy dołączyć do jej akt osobowych. Dokumenty aplikacyjne pozostałych osób biorących udział w naborze, należy przechowywać przez okres nieprzekraczający 3 miesięcy od dnia nawiązania stosunku pracy z osobą wyłonioną w drodze naboru, na wypadek wystąpienia konieczności ponownego obsadzenia tego samego stanowiska. Możliwe jest zatrudnienie na tym samym stanowisku innej osoby spośród najlepszych kandydatów wyłonionych przez komisję w toku naboru na wolne stanowisko urzędnicze, w tym kierownicze. Po upływie tych 3 miesięcy dokumenty aplikacyjne pozostałych osób biorących udział w naborze należy zniszczyć. Dokumentacja posiedzeń komisji z naboru powinna być przechowywana zgodnie z kategorią archiwalną wynikającą z JRWA (B2). W przypadku konkursów na stanowiska (dot. pracowników pedagogicznych), dokumenty aplikacyjne osoby zatrudnionej należy dołączyć do jej akt osobowych, natomiast dokumenty kandydatów niezatrudnionych w przypadku braku ich zgody na przetwarzanie danych na potrzeby przyszłych rekrutacji, należy niezwłocznie usunąć. Dokumentacja posiedzeń komisji archiwizuje się zgodnie z kategorią archiwalną A/B25*(stosować odpowiednio w zależności od tego, czy jednostka oświatowa wytwarza dokumentację kwalifikującą się do materiałów archiwalnych (kat A), tj. została uznana za jednostkę wytwarzającą materiały archiwalne przez miejscowo właściwe archiwum państwowe). Dokumentacja aplikacyjna wybranego kandydata do pracy, zostaje dołączona do jego akt osobowych i jest archiwizowana przez okres 10 lat, a w przypadku pracowników zatrudnionych przed dniem 1 stycznia 2019 r. przez okres 50 lat od dnia ustania stosunku pracy. W przypadku, gdy do szkoły wpłyną dokumenty

		aplikacyjne nadesłane poza ogłoszeniami o naborze, należy zweryfikować czy kandydat w nadesłanej dokumentacji aplikacyjnej wyraził zgodę na przetwarzanie danych osobowych dla celów prowadzenia przyszłych procesów rekrutacyjnych. W takim przypadku, dokumenty mogą być przechowywane. W przypadku gdy dokumenty aplikacyjne zostaną złożone bez zgody na przetwarzanie danych osobowych dla celów prowadzenia przyszłych procesów rekrutacyjnych, z punktu widzenia ochrony danych osobowych nie powinny być one przechowywane. Brak jest podstaw do tego aby stosować do nich JRWA Jednostek oświatowych miasta Lublin. Zatem, dokumenty aplikacyjne powinny być niszczone w sposób i w terminach wynikających z regulacji wewnętrznych. Powyższe będzie miało zastosowanie do dokumentów aplikacyjnych złożonych: poza ogłoszeniami o naborze, po terminie określonym w ogłoszeniu o naborze a także złożonych bez podania nazwy stanowiska zamieszczonego w ogłoszeniu o naborze. Szkoła po otrzymaniu ww. dokumentów, niezawierających zgody na przetwarzanie danych na potrzeby przyszłych naborów, może wystąpić do wnioskodawcy uzupełnienie wniosku tj. wyrażenie zgody na przetwarzanie danych w określonym okresie, ustalonym przez Dyrektora szkoły

d) Zabezpieczenia systemu teleinformatycznego

Kryterium nr 1 **stosowanie zabezpieczeń danych chronionych zapewniających poufność oraz przeciwdziałających dostępowi osób nieupoważnionych**	**Czy są stosowane adekwatne zabezpieczenia danych chronionych?** W sytuacji gdy jednocześnie spełnione są wszystkie następujące warunki: -wiadomości e-mail, zawierające dane chronione wysyłane za pomocą e-mail są szyfrowana (pliki z danymi chronionymi są zaszyfrowane), a hasło przekazywane jest inną drogą komunikacji iż wiadomości -dane chronione przechowywane na przenośnych nośnikach danych są szyfrowane -ekran monitora jest blokowany po zakładanym czasie bezczynności komputera (np., określonym w regulacjach jednostki) -hasło dostępowe do komputera jest regularnie zmieniane oraz spełnia wymogi dotyczące jego złożoności wówczas : 80 % i więcej badanych przypadków – **kryterium spełnione** 50-79 % – **kryterium spełnione częściowo** poniżej 50 % - **kryterium niespełnione**

Ustalenia	Ocena zgodności	Rekomendacje
1.**Poczta elektroniczna**: a) Próba kontroli – 21 kont poczty ustalenie – poczta częściowo jest hostowana przez UML, 10 kont pocztowych hostowanych jest przez UML, natomiast 11 kont pocztowych hostowanych jest samodzielnie przez Szkołę. b) próba kontroli – 9 użytkowników a. W jednym przypadku (11%) obsługa poczty w szkole odbywała się za pomocą aplikacji RoundCube oraz klienta poczty Microsoft Outlook 2013. We wszystkich pozostałych przypadkach (89%) obsługa poczty odbywała się za pomocą aplikacji RoundCube oraz na stronie poczta.g16-lublin.eu. W jednym przypadku nie realizowano wymogu konieczności każdorazowego podawania danych autoryzacyjnych (login i hasło) podczas logowania do poczty elektronicznej za pomocą aplikacji RoundCube (dane autoryzacyjne zapisane były w pamięci przeglądarki). Podczas sprawdzenia dokonano jednak korekty w tym zakresie i usunięto z pamięci przeglądarki zapamiętane dane autoryzacyjne do logowania. b. na 7 z 21 zweryfikowanych skrzynek nadawczych (33%) wysłana korespondencja zawierała dane chronione, które nie były zaszyfrowane przed jej wysłaniem. 2.**System operacyjny**. Próba kontroli – 9 jednostek roboczych: a) na 4 komputerach (44%) wygaszacz ekranu nie był skonfigurowany zgodnie z wymogami RSI, b) hasła dostępowe do systemu Windows na wszystkich sprawdzanych komputerach (100%) spełniały wymogi złożoności, długości i cykliczności zmiany, c) na wszystkich sprawdzanych komputerach (100%) realizowano wymóg konieczności każdorazowego podawania danych autoryzacyjnych (login i hasło) podczas logowania do systemu operacyjnego. 3.**Szyfrowanie danych**. W szkole użytkowany jest tylko jeden komputer przenośny, który jest wykorzystywany przez pracownika BHP. Ustalono, że przenośny wewnętrzny nośnik danych w tym komputerze nie został zaszyfrowany. Ponadto, zgodnie z wyjaśnieniami pracowników, w szkole wykorzystywane są dwa przenośne zewnętrzne nośniki danych. Oba były zaszyfrowane: a) pendrive użytkowany przez sekretarkę. Pamięć jest zaszyfrowana przy użyciu funkcji BitLocker w Windows 10 (hasło do odszyfrowania zna sekretarka) i przechowywana w zamykanej na klucz metalowej szafie w sekretariacie. Jest ona nośnikiem dokumentów wykorzystywanych przez sekretarkę do codziennej pracy, zawiera dane osobowe (dane uczniów szkoły SP nr 16),	Kryterium spełnione częściowo	1. Korzystać wyłącznie z poczty hostowanej przez UML. 2. Zapewnić poufność danych chronionych przekazywanych przez pocztę elektroniczną. Hasła do zaszyfrowanej korespondencji przekazywać poprzez inne kanały komunikacji niż poczta np. telefonicznie lub osobiście. 3. Szyfrować dane przechowywane na nośnikach przenośnych. 4. Wprowadzić na stacjach roboczych blokadę wygaszaczem ekranu. 5. Przeprowadzić szkolenie dla użytkowników z zakresu bezpieczeństwa teleinformatycznego, zwłaszcza w kontekście zasad uwierzytelniania (za pomocą identyfikatorów i haseł oraz przechowywania haseł). 6. Zabezpieczyć pocztę elektroniczną poprzez wprowadzenie wymogu każdorazowego logowania (podanie loginu i hasła). **Termin realizacji: 30.06.2020r** **Osoba odpowiedzialna**: Marcin Zmysłowski (ASI)

b) pendrive użytkowany przez kierownika gospodarczego, który przeznaczony jest do przechowywania plików z nagraniami z kamer monitoringu szkolnego (brak kopii zapasowych z nagrań w dniu sprawdzenia). Pamięć jest zaszyfrowana przy użyciu funkcji BitLocker w Windows 10 (hasło do odszyfrowania zna ochroniarz szkolny) i przechowywana w zamykanej na klucz metalowej szafie w sekretariacie (jest to ta sama szafa, w której znajduje się pendrive sekretarki).		

Kryterium nr 2 **stosowanie wymaganych zabezpieczeń na stacjach roboczych**	**Czy na stacjach roboczych stosowane są zabezpieczenia wymagane w SZBI?** Kryteria oceny: W sytuacji gdy na stacjach roboczych/serwerów jednocześnie spełnione są wszystkie następująca warunki: -zainstalowana jest aktualna wersja oprogramowania antywirusowego (aktualna baza wirusów i silnik programu), -system operacyjny jest aktualny (aktualizacje krytyczne), -uruchomiona jest zapora ogniowa (firewall), -dostęp do BIOS zabezpieczony jest hasłem, -jedynym nośnikiem bootującym (uruchamiającym) system operacyjny jest dysk twardy. wówczas : 80 % i więcej komputerów spełnia ww. warunki – **kryterium spełnione** 50-79 % – **kryterium spełnione częściowo** poniżej 50 % - **kryterium niespełnione**

Ustalenia	Ocena zgodności	Rekomendacje
Próba kontroli - 9 jednostek roboczych. 1. Wszystkie sprawdzane komputery (100%) posiadały aktualną wersję oprogramowania antywirusowego. 2. Wszystkie sprawdzane komputery (100%) posiadały włączoną zaporę ogniową. 3. System operacyjny zainstalowany na 4 z 9 sprawdzanych komputerów (44%) był nieaktualny (aktualizacje krytyczne nie były zainstalowane). 4. Wszystkie sprawdzane komputery (100%) posiadały zabezpieczony hasłem dostęp do BIOS. 5. Wszystkie sprawdzane komputery (100%) posiadały w konfiguracji BIOS dysk twardy (wewnętrzny nośnik danych) jako pierwszy nośnik uruchamiania systemu operacyjnego.	Kryterium spełnione częściowo	Na stacjach roboczych zapewnić stosowanie zabezpieczeń wymaganych w RSI. **Termin realizacji: 30.06.2020r.** **Osoba odpowiedzialna:** Marcin Zmysłowski (ASI)

Kryterium nr 3 **zapewnienie rozliczalności użytkowników systemów administrowanych przez Jednostkę.**	**Czy zapewniono rozliczalność użytkowników w systemach administrowanych przez Jednostkę?** Kryteria oceny: 80 % i więcej użytkowników posiada w systemach jednostki identyfikatory umożliwiające rozliczalność - **kryterium spełnione** 50 % - 79 % użytkowników posiada w systemach jednostki identyfikatory umożliwiające rozliczalność - **kryterium spełnione częściowo** mniej niż 50 % użytkowników posiada w systemach jednostki identyfikatory umożliwiające rozliczalność - **kryterium niespełnione**		
Ustalenia		**Ocena zgodności**	**Rekomendacje**
1. **Poczta elektroniczna**. Próba kontroli – 21 kont poczty. W 3 z 21 przypadków (14%) nie zapewniono rozliczalności, ponieważ na konta: poczta@sp16.lublin.eu, szkola@g16-lublin.eu, poczta@g16-lublin.eu, pracownik sekretariatu logował się bezpośrednio a nie na swoje konto indywidualne i za jego pośrednictwem na tożsamość kont technicznych. 2. **System operacyjny** Próba kontroli – 9 komputerów. Na wszystkich komputerach (100%) zapewniono rozliczalność – utworzone zostały imienne konta dla wszystkich użytkowników. 3. **System monitoringu** Żadne z utworzonych kont w systemie monitoringu nie zapewnia rozliczalności, tj.: - admin (konto wbudowane z uprawnieniami administracyjnymi) założone na rejestratorze nr 1, 2, 3, 4, 5, 6, - ochrona (konto z uprawnieniami standardowymi) założone na rejestratorze nr 1, 2, 3, 4, 5. Konto jest wykorzystywane przez pracownika ochrony oraz stróża nocnego, - kierownik (konto z uprawnieniami administracyjnymi) założone na rejestratorze nr 1, 2, 3, 4, 6, -serwis (konto z uprawnieniami administracyjnymi) założone na rejestratorze nr 5. Zgodnie z wyjaśnieniami kierownika gospodarczego, który sprawuje obsługę informatyczną systemu konto serwis nie jest użytkowane.	Kryterium niespełnione	Zapewnić rozliczalność użytkowników w systemach poczty elektronicznej i monitoringu. **Termin realizacji: 30.06.2020r.** **Osoba odpowiedzialna:** Marcin Zmysłowski (ASI) i Jarosław Kasperek (kierownik gospodarczy)

Kryterium nr 4 **zapewnienie właściwych poziomów dostępów do systemu teleinformatycznego oraz właściwe zabezpieczenie administracyjnych danych dostępowych**	**Pracownicy nie będący ASI posiadają konta dostępowe do systemu teleinformatycznego z ograniczonymi uprawnieniami oraz hasła administracyjne zostały właściwe zabezpieczone i zdeponowane?** Kryteria oceny 80 % i więcej użytkowników posiada konta z ograniczeniami – **kryterium spełnione** 50-79 % – **kryterium spełnione częściowo** poniżej 50 % - **kryterium niespełnione** **W przypadku gdy hasła administracyjne do elementów systemu teleinformatycznego nie są zdeponowane w sposób zapewniający ich bezpieczeństwo oraz dostęp do nich przez KJO, niezależnie od wyników oceny kryterium uznane będzie za niespełnione.**

Ustalenia	Ocena zgodności	Rekomendacje
1. **System operacyjny** – Próba kontroli - 9 komputerów. Konta użytkowników na wszystkich sprawdzanych komputerach (100%) były prawidłowo skonfigurowane – miały uprawnienia ograniczone. **2. System monitoringu** Dostęp do systemu monitoringu na poziomie administracyjnym posiada dyrektor szkoły, administrujący tym systemem kierownik gospodarczy jak również pracownik ochrony. Nadanie dostępu administracyjnego pracownikowi ochrony, jest w opinii BI bezzasadne. **3. Zabezpieczenie dostępowych danych administracyjnych.** Dostępowe dane administracyjne (hasła administracyjne) nie były zabezpieczone prawidłowo, ponieważ: - hasła administracyjne do Active Directory, wszystkich serwerów bazujących na systemie Linux, routera brzegowego oraz do BIOS-ów stacji roboczych, do NAS zostały wprawdzie zdeponowane w sejfie znajdującym się w sekretariacie, jednak dostęp do niego posiadała osoba nieuprawniona (pracownik sekretariatu). - hasła administracyjne do systemu monitoringu były zdeponowane u kierownika gospodarczego. W trakcie sprawdzenia wszystkie ww. hasła zdeponowano w kasetce, którą umieszczono w pokoju dyrektora. - hasło administracyjne do hostingu w ogóle nie zostało zdeponowane. **Dodatkowo ustalono, że:** 1. W szkole zdeponowano hasła wszystkich użytkowników do poczty elektronicznej oraz systemu monitoringu pomimo, że są to dane które powinny być znane tylko poszczególnym użytkownikom. 2. Użytkownicy przechowują hasła w miejscach niezabezpieczonych (np. w prywatnych notatnikach lub kartce papieru) – zalecenie w tym zakresie wydano w kryterium nr 1.	Kryterium niespełnione	1. Zapewnić właściwe poziomy dostępu dla użytkowników systemu monitoringu. 2. Hasła administracyjne do wszystkich systemów teleinformatycznych zabezpieczyć i zdeponować zgodnie z wymogami RSI. 3. Zniszczyć zdeponowane indywidualne hasła użytkowników do poczty elektronicznej i systemu monitoringu. 4. Nie pobierać od użytkowników haseł dostępowych do systemów teleinformatycznych. **Termin realizacji: 30.06.2020r.** **Osoba odpowiedzialna:** Marcin Zmysłowski (ASI) i Jarosław Kasperek (kierownik gospodarczy)

Kryterium nr 5 zapewnienie zasilania awaryjnego	**Czy zapewniono zasilenie awaryjne kluczowych stacji roboczych/ serwerów lub innych kluczowych elementów systemu teleinformatycznego?** Kryteria oceny: 80 % i urządzeń posiada zasilanie awaryjne– **kryterium spełnione** 50-79 % – **kryterium spełnione częściowo** poniżej 50 % - **kryterium niespełnione**		
Ustalenia		**Ocena zgodności**	**Rekomendacje**
Zasilanie awaryjne kluczowych elementów ST – Weryfikacja 21 kluczowych elementów: 11 aktywnych urządzeń sieciowych, 2 serwery, 1 termostat, 6 rejestratorów obrazu z kamer monitoringu i 74 kamery rejestrujące obraz (traktowane jako całość i jeden kluczowy element systemu teleinformatycznego). Ustalenie: dla 8 z 21 (38%) kluczowych elementów systemu teleinformatycznego nie zapewniono zasilania awaryjnego. Szczegółowe ustalenia: Kluczowe urządzenia znajdują się w dwóch pomieszczeniach (serwerowni oraz pomieszczeniu gdzie umieszczono urządzenia rejestrujące i podglądu w systemie monitoringu wizyjnego). 1. Serwerownia: a) termostat - zapewniono zasilanie awaryjne, b) switch - zapewniono zasilanie awaryjne, c) dysk sieciowy NAS służący do wykonywania backupów - zapewniono zasilanie awaryjne, d) dysk sieciowy NAS będący źródłem przestrzeni dyskowej dla serwera - zapewniono zasilanie awaryjne, e) serwer terminali dla pracowni informatycznych - zapewniono zasilanie awaryjne, f) serwer maszyn wirtualnych - zapewniono zasilanie awaryjne, g) switch Cisco - zapewniono zasilanie awaryjne, h) router brzegowy - zapewniono zasilanie awaryjne, i) switch z podpiętym światłowodem - zapewniono zasilanie awaryjne, j) switch z łączem od zewnętrznego dostawcy - zapewniono zasilanie awaryjne, k) trzy switche, które rozprowadzają sieć po pracowniach informatycznych – zapewniono zasilanie awaryjne, l) firewall Palo Alto – nie zapewniono zasilania awaryjnego. 2. Pomieszczenie monitoringu: a) 6 rejestratorów monitoringu wizyjnego – nie zapewniono zasilania awaryjnego, b) kamery monitoringu - nie zapewniono zasilania awaryjnego.		Kryterium spełnione częściowo	Zapewnić zasilanie awaryjne dla firewalla Palo Alto oraz rejestratorów obrazu z kamer monitoringu szkolnego i samych kamer. **Termin realizacji: w miarę posiadanych środków finansowych.** **Osoba odpowiedzialna:** Marcin Zmysłowski (ASI)

Kryterium nr 6 **zabezpieczenia zapewniające zdolność do szybkiego przywrócenia dostępności danych w razie incydentu**	**Czy zapewniona jest zdolność do szybkiego przywrócenia dostępności danych w razie incydentu zgodnie z wymogami SZBI?** Kryteria oceny: W przypadku gdy kopie zapasowe wykonywane są z częstotliwością: do 1 tygodnia - **kryterium spełnione** w przedziale powyżej tygodnia do 1 miesiąca - **kryterium spełnione częściowo** rzadziej niż co 1 miesiąc lub wcale – **kryterium niespełnione** **W sytuacji gdy kopie zapasowe przechowywane są na tym samym dysku fizycznym komputera/serwera na którym są wykonywane niezależnie od częstotliwości ich wykonywania – kryterium niespełnione**

Ustalenia	Ocena zgodności	Rekomendacje
1. ASI realizuje kopie zapasowe będące obrazami całych maszyn wirtualnych. Kopie te realizowane są automatycznie, codziennie przyrostowo przez Veem Backup and Replication na dysku sieciowym NAS, który znajduje się w tej samej szafie teleinformatycznej, w której znajduje się serwer, z którego wykonywane są kopie zapasowe (szafa teleinformatyczna nr 1 ujęta w arkuszu sprawdzenia). Wykonywanie kopii zapasowych nie jest dokumentowane zgodnie z wymogami SZBI, ponieważ ASI nie sporządza harmonogramu wykonywania kopii. 2. Kopie zapasowe z programu kadrowego, księgowego i płacowego realizowane są przez Wydział IT i znajdują się w Miejskim Centrum Przetwarzania Danych.	Kryterium niespełnione	1. Kopie zapasowe maszyn wirtualnych przechowywać w innej lokalizacji niż urządzenie, z którego są wykonywane. 2. Na bieżąco prowadzić harmonogram wykonywania kopii zapasowych zgodny z Załącznikiem nr 3 do RSI. **Termin realizacji: w miarę posiadanych środków finansowych.** **Osoba odpowiedzialna: Marcin Zmysłowski (ASI)**

Kryterium nr 7 **legalność oprogramowania zainstalowanego na komputerach oraz zgodność plików multimedialnych z wymogami SZBI**	**Czy zainstalowane na komputerach aplikacje wymagające licencji są ujęte w ewidencji oprogramowania oraz są zainstalowane zgodnie z postanowieniami licencji? Czy pliki multimedialne znajdujące się na komputerach są związane z wykonywaniem obowiązków służbowych?** Kryteria oceny: na 80 % i więcej komputerach aplikacje wymagające licencji są ujęte w ewidencji oprogramowania i są zainstalowane zgodnie z postanowieniami licencji oraz pliki multimedialne znajdujące się na tych komputerach są związane z wykonywaniem obowiązków służbowych - **kryterium spełnione** 50-79 % – **kryterium spełnione częściowo** poniżej 50 % - **kryterium niespełnione**

Ustalenia	Ocena zgodności	Rekomendacje
Próba kontroli - 9 komputerów. 1. Na wszystkich sprawdzanych komputerach objętych sprawdzeniem (100%), oprogramowanie wymagające licencji było zainstalowane zgodnie z jej postanowieniami. 2. W jednostce prowadzona jest ewidencja oprogramowania w sposób niezgodny z tym, który określony jest w SZBI, tj. ewidencja nie zawiera informacji określającej: użytkownika oprogramowania, czas trwania licencji oraz wersję oprogramowania. 3. Na 1 z 9 sprawdzanych komputerów (11%) znajdowały się pliki multimedialne, które nie były związane z wykonywaniem obowiązków służbowych, tzn. kilkanaście plików mp3.	Kryterium spełnione	1. Prowadzić ewidencję oprogramowania w sposób zgodny z SZBI. 2. Nie przechowywać na komputerach plików multimedialnych, które nie są związane z wykonywaniem obowiązków służbowych. **Termin realizacji: 30.06.2020r.** **Osoba odpowiedzialna:** Marek Gielara (ASI)

Kryterium nr 8 stosowanie odpowiednich zabezpieczeń w pomieszczeniu serwerowni	**1. Czy w pomieszczeniu serwerowni zastosowano drzwi antywłamaniowe i przeciwpożarowe, jeżeli wyniki szacowania ryzyka wskazują na takie zabezpieczenie?** **2. Czy w pomieszczeniu serwerowni zastosowano system alarmowy przeciwwłamaniowy?** **3. Czy prowadzona jest ewidencja wejść i wyjść osób nie będących Informatykami?** **4. Czy w pomieszczeniu serwerowni zastosowano czujnik dymu wraz z możliwością alarmowania?** **5. Czy w pomieszczeniu serwerowni znajduje się gaśnica spełniająca wymagania gaszenia urządzeń elektrycznych?** **6. Czy zastosowano zamykane na klucz metalowe szafy teleinformatyczne przeznaczone dla urządzeń pracujących w serwerowni?** **Kryteria oceny:** 80 % i więcej elementów zrealizowanych - **kryterium spełnione** 50-79 % elementów zrealizowanych - **kryterium spełnione częściowo** poniżej 50 % elementów zrealizowanych - **kryterium niespełnione**

Ustalenia	Ocena zgodności	Rekomendacje
Sprawdzeniu podlegało pomieszczenie serwerowni. Ustalenie: 1. Drzwi wejściowe do serwerowni są antywłamaniowe, ale nie przeciwpożarowe. Zastosowano system alarmowy przeciwwłamaniowy oraz czujnik dymu wraz z możliwością alarmowania. W serwerowni znajduje się gaśnica spełniająca wymagania gaszenia urządzeń elektrycznych. Zastosowano także zamykane na klucz metalowe szafy teleinformatyczne przeznaczone dla urządzeń pracujących w serwerowni (łącznie trzy szafy dla wszystkich urządzeń). 2. Nie jest prowadzona ewidencja wejść i wyjść osób nie będących Informatykami	Kryterium spełnione częściowo	1. Zastosować w serwerowni drzwi antywłamaniowe i przeciwpożarowe. 2. Prowadzić w serwerowni ewidencję wejść i wyjść osób nie będących Informatykami. **Termin realizacji: W miarę posiadanych środków finansowych.** **Osoba odpowiedzialna: Jarosław Kasperek (kierownik gospodarczy)**
		Sporządzili: *Katarzyna Skowyra* *Aleksander Czubacki* *Sprawdzili:* *Grzegorz Tymecki* *Tomasz Pałysewicz* *Zatwierdził:* *Witold Przeszlakowski*

IV. Wykaz aktów prawnych

1. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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);
2. **Kodeks Pracy** – Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 2019 poz. 1040);
3. **Prawo Oświatowe** – Ustawa z dnia 14 grudnia 2016 r. (Dz. U. 2019 poz 1148);
4. **Ustawa o pracownikach samorządowych** – Ustawa z dnia 21 listopada 2008 r. (Dz. U. 2019 r. poz. 1282);
5. **UoKSC** - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
6. **KRI** - Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
7. **Minimalne wymogi dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostkach organizacyjnych Gminy Lublin** – Zarządzenie nr 65/4/2018 Prezydenta Miasta Lublin z dnia 20 kwietnia 2018 r.
8. **JRWA** - Zarządzenie nr 75/4/2017 Prezydenta Miasta Lublin z dnia 19 kwietnia 2017r. w sprawie wprowadzenia normatywów kancelaryjno-archiwalnych w jednostkach oświatowych miasta Lublin z późn. zm. na podstawie Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. 2011 nr 14 poz. 67);

V. Słownik

1. **SZBI** – System Zarządzania Bezpieczeństwem Informacji
2. **PBI** – Polityka Bezpieczeństwa Informacji
3. **RBI** – Regulamin Bezpieczeństwa Informacji
4. **RSI** – Regulamin Systemu Informatycznego
5. **UODO** – Urząd Ochrony Danych Osobowych
6. **IOD** – Inspektor Ochrony Danych Osobowych
7. **ASI** – Administrator Systemu Informatycznego
8. **JOM** – jednostki organizacyjne Miasta Lublin
9. **RCP** – rejestr czynności przetwarzania
10. **RUP** – rejestr umów powierzenia
11. **RKP** - rejestr kategorii przetwarzania
12. **AR** – analiza ryzyka