Audyt wewnętrzny jednostki na podstawie Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. z 2024 r. poz. 773

Poz.	Obszar / Obszar szczegółowy / Wymaganie	Podstawa prawna	Kontroli podlegają	Dokumenty potwierdzające spełnienie wymagania*)	Uwagi i wyjaśnienia*)	Samoocena spełnienia wymagania *) S/N/CS/ND	Komórka i osoba udzielająca odpowiedzi *)	nr telefonu do osoby udzielającej odpowiedzi*)
1	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	**Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną**							
1.1	**Usługi elektroniczne**							
1.1.1	Czy Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę? Czy interoperacyjność na poziomie organizacyjnym osiągana jest przez: - informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty, - publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną?	*art. 16 ust. 1a ustawy o informatyzacji* *§ 5 ust. 2 pkt 1 rozporządzenia KRI* *§ 5 ust. 2 pkt 4 rozporządzenia KRI*	Świadczenie usług w formie elektronicznej z wykorzystaniem ESP Zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP podmiotu), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw.	Na stronie głównej Zespołu Szkół Leśnych w Leskuhttps://www.zsllesko.pl udostępniono link do funkcjonalności ePUAP https://epuap.gov.pl/wps/portal/strefaklienta/katalog-spraw/profil-urzedu/zsllesko	brak	S	Wicedyrektor	509619849
1.2	**Centralne repozytorium wzorów dokumentów elektronicznych**							

1.2.1	Czy organ administracji publicznej przekazuje do centralnego repozytorium (prowadzonego w ramach ePUAP przez Ministra właściwego do spraw informatyzacji) oraz udostępnia w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych?	*art. 19b ust. 3 ustawy o informatyzacji*	• Wykorzystanie przez jednostkę wzorów dokumentów elektronicznych przechowywanych w CRWDE, jakie zostały już wcześniej opracowane i są używane przez inny urząd. • Przekazanie do CRWDE oraz udostępnienie w BIP wzorów dokumentów elektronicznych.	Szkoła nie wprowadziła własnych wzorów dokumentów umieszczonych w Centralnym Repozytorium Wzorów Dokumentów Elektronicznych	brak	N	Wicedyrektor	509619849
1.3	**Model usługowy**							
1.3.1	Czy zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury?	*§ 15 ust. 2 rozporządzenia KRI*	• Poziom wspierania modelu usługowego w procesie świadczenia usług elektronicznych przez systemy teleinformatyczne podmiotu. • Weryfikacja sposobu zarządzania usługami w oparciu o ustalone procedury, w tym: możliwość zidentyfikowania właściciela merytorycznego usług (komórka organizacyjna podmiotu), ustalenie odpowiedzialności za utrzymanie usług od strony technicznej, określenie poziomu świadczenia usług, monitorowanie poziomu świadczenia usług na zadeklarowanym poziomie.	Nie określono procedury.	brak	N	Wicedyrektor	509619849
1.4.	**Współpraca systemów teleinformatycznych z innymi systemami**							
1.4.1	Czy interoperacyjność na poziomie semantycznym osiągana jest przez stosowanie w rejestrach prowadzonych przez podmioty od wołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań? Czy systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej?	*§ 5 ust. 3 pkt 3 rozporządzenia KRI* *§ 16 ust. 1 rozporządzenia KRI*	• Poziom współpracy systemów teleinformatycznych z innymi systemami podmiotu lub systemami informatycznymi innych urzędów w tym rejestrami referencyjnymi. • Sposób komunikacji z innymi systemami, w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających bezpieczeństwo informacji.	System wyposażony jest w infrastrukturę pozwalającą wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach.	brak	S	Wicedyrektor	509619849
1.5	**Obieg dokumentów w jednostce**							

1.5.1	Czy zapewniono zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie?	*§ 19 ust. 2 pkt 9 rozporządzenia KRI*	• Regulacje wewnętrzne opisujące sposób zarządzania obiegiem dokumentów w podmiocie, w tym zakres stosowania elektronicznego obiegu dokumentów.	W jednostce obowiązuje podstawowy tradycyjny („papierowy") obieg dokumentów wspomagany dziennikiem elektronicznym. Jednostka posiada regulacje wewnętrzne dot. Instrukcji kancelaryjnej, polityki przetwarzania danych osobowych, nadawania uprawnień itp.	brak	S	Wicedyrektor	509619849

1.6	**Formaty danych udostępniane przez systemy teleinformatyczne**							
1.6.1	Czy kodowanie znaków w dokumentach wysyłanych z systemu teleinformatycznego także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą? Czy system teleinformatyczny udostępnia zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia KRI? Czy system teleinformatyczny umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu działania podmiotu w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia KRI - jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej?	*§ 17 ust.1 rozporządzenia KRI § 18 ust 1 rozporządzenia KRI § 18 ust. 2 rozporządzenia KRI*	• Potwierdzenie sposobu kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu. • Potwierdzenie sposobu udostępniania zasobów informatycznych z systemów teleinformatycznych podmiotu. • Potwierdzenie sposobu przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne podmiotu.	Stosowane formaty są zgodne z wymaganiami zawartymi w KRI	brak	S	Wicedyrektor	509619849
2	**System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych**							
2.1	**Dokumenty z zakresu bezpieczeństwa informacji, Zaangażowanie kierownictwa podmiotu**							

2.1.1	Czy opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji (SZBI) zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność?	*§ 19 ust. 1 rozporządzenia KRI* *§ 19 ust. 2 rozporządzenia KRI*	• Dokumentacja SZBI w tym Polityka Bezpieczeństwa Informacji oraz inne dokumenty stanowiące SZBI, w tym m.in.: PBI, dokumentacja przeglądów SZBI, dokumentacja szacowania ryzyka, audyty, dokumentacja incydentów naruszenia BI. • Stopień zaangażowania kierownictwa podmiotu publicznego w proces ustanawiania Bezpieczeństwa Informacji.	Jednostka wdrożyła w grudniu 2024 r. .dokumentację SZBI a Polityka Bezpieczeństwa Informacji/ funkcjonuje od 2018 r. wdrożona Zarządzenie nr 01/V/2018 z dnia 25.05.2018 oraz . dokumentację dotycząca przetwarzania danych osobowych zgodną z RODO.(2018)	brak	S	Wicedyrektor	509619849
2.1.2	Czy SZBI jest monitorowany, poddawany przeglądom oraz doskonalony? Czy zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizacje i egzekwowanie działań związanych z SZBI? Czy regulacje wewnętrzne w zakresie SZBI są aktualizowane w zakresie dotyczącym zmieniającego się otoczenia?	*§ 19 ust. 1 rozporządzenia KRI* *§ 19 ust. 2 pkt 1 rozporządzenia*	• Działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników analizy ryzyka, wniosków z przeglądów SZBI, zaleceń po audytowych, wniosków z analizy incydentów naruszenia SZBI. • Stopień zaangażowania kierownictwa podmiotu publicznego w proces zarządzania SZBI, (przeglądy SZBI, egzekwowanie działań związanych z BI).	Dokumentacja SZBI jest monitorowana, poddawana przeglądom, aktualizowana.	brak	S	Wicedyrektor	509619849
2.2	**Analiza zagrożeń związanych z przetwarzaniem informacji**							

2.2.1	Czy przeprowadzana jest okresowa analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz czy podejmowane są działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy?	*§ 19 ust. 2 pkt 3 rozporządzenia KRI*	• Regulacje wewnętrzne opisujące sposób zarządzania ryzykiem SZBI. Dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyka, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, sposobie postępowania z ryzykami oraz plan postępowania z ryzykiem. • • Działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem, stosownie do analizy ryzyka.	Przeprowadza się analizy ryzyka. Wykonuje się także analizę rozwiązań informatycznych mających na celu podniesienie poziomu bezpieczeństwa	brak	S	Wicedyrektor	509619849
2.3	**Inwentaryzacja sprzętu i oprogramowania informatycznego**							

2.3.1	Czy utrzymywana jest aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację?	*§ 19 ust. 2 pkt 2 rozporządzenia KRI*	• Regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych (bazą danych zarządzania konfiguracją CMDB). • Rejestr zasobów teleinformatycznych (baza konfiguracji CMDB) zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. • Sposób aktualizacji rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB).	Dokumentacja SZBI zawiera procedury zarządzania sprzętem informatycznym, Inwentaryzacja sprzętu wykonywana jest w wersji cyfrowej w dedykowanym programie nVision (Axence.net),„papierowo" na potrzeby rachunkowości.	brak	S	Wicedyrektor	509619849
2.4	**Zarządzanie uprawnieniami do pracy w systemach informatycznych**							
2.4.1	Czy osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji? Czy zakres uprawnień osób zaangażowanych w przetwarzanie danych jest bezzwłocznie zmieniany, w przypadku zmiany zadań tych osób?	*§ 19 ust. 2 pkt 4 rozporządzenia KRI* *§ 19 ust. 2 pkt 5 rozporządzenia KRI*	• Regulacje wewnętrzne opisujące zarządzanie uprawnieniami użytkowników do pracy w systemach teleinformatycznych w tym do przetwarzania danych osobowych. • Adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień). • Działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.	Pracownicy posiadają stosowne uprawnienia do systemów i zasobów na podstawie dokumentacji ochrony danych osobowych oraz ról w SZBI.	brak	S	Wicedyrektor	509619849

			• Sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych					
2.5	**Szkolenia pracowników zaangażowanych w proces przetwarzania informacji**							

2.5.1	Czy zapewniono szkolenie osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich?	*§ 19 ust. 2 pkt 6 rozporządzenia KRI*	• Regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych. • Dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń.	Brak szkoleń po dniu 21 maja 2024 r. (wprowadzeniu KRI). Zapewniono szkolenia pracowników w 2018 r. Po wprowadzeniu RODO.	brak	CS	Wicedyrektor	509619849
2.6	**Praca na odległość i mobilne przetwarzanie danych**							
2.6.1	Czy ustanowiono podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość?	*§19 ust. 2 pkt 8 rozporządzenia KRI*	• Regulacje wewnętrzne, w których określono zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość. • Działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość.	Ustanowiono procedury wewnętrzne w SZBI oraz dokumentacji RODO.	brak	S	Wicedyrektor	509619849
2.7	**Serwis sprzętu informatycznego i oprogramowania**							
2.7.1	Czy umowy serwisowe podpisane ze stronami trzecimi zawierają zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji?	*§19 ust. 2 pkt 10 rozporządzenia KRI*	• Regulacje wewnętrzne, w których określono zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych, w tym wymagane klauzule prawne dotyczące SZBI. • Umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI.	Ustanowiono procedury wewnętrzne w SZBI oraz dokumentacji RODO. Umowy zapewniają odpowiedni poziom bezpieczeństwa.	brak	S	Wicedyrektor	509619849
2.8	**Procedury zgłaszania incydentów naruszenia BI**							

2.8.1	Czy incydenty naruszenia bezpieczeństwa informacji są bezzwłocznie zgłaszane w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących?	*par. 19 ust. 2 pkt 13 rozporządzenia KRI*	• Regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji. • Sposób zgłaszani i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CSIRT.	Ustanowiono regulacje wewnętrzne w dokumentacji SZBI i ochrony danych osobowych , brak wyznaczonej osoby do kontaktów z CSIRT. Brak analizy logów, brak analiz zagrożeń wynikający z braku etatowego informatyka. Reakcja na incydenty jest prawidłowa.	brak	N	Wicedyrektor	509619849
2.9	**Audyt wewnętrzny z zakresu bezpieczeństwa informacji**							
2.9.1	Czy przeprowadzany jest audyt wewnętrzny w zakresie SZBI co najmniej raz w roku?	*§ 19 ust. 2 pkt 14 rozporządzenia KRI*	• Regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie SZBI. • Sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji. • Działania podjęte w wyniku zaleceń po audytowych.	Dokumentacja SZBI zawiera „Procedurę przeprowadzania audytów wewnętrznych". W 2023 r. nie przeprowadzano audytów, audyt za rok 2024 przeprowadzono w grudniu 2024.	brak	S	Wicedyrektor	509619849
2.10	**Kopie zapasowe**							
2.10.1	Czy zapewniono odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegający w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.	*§ 19 ust. 2 pkt 12 lit. b rozporządzenia KRI*	• Regulacje wewnętrzne, w których określono zasady tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu. • Działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja tych działań.	Dokumentacja SZBI zawiera regulacje wewnętrzne związane z tworzeniem, testowaniem i przechowywaniem kopii zapasowych. Procedury takie zawiera także dokumentacja ochrony danych osobowych. Część danych /dziennik elektroniczny/ posiada odrębne procedury tworzenia kopii zapasowych. Nie wszystkie zbiory danych posiadają backupy.	brak	CS	Wicedyrektor	509619849
2.11	**Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych**							

2.11.1	Czy systemy teleinformatyczne zostały zaprojektowane, wdrożone i eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenaszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.	*§ 15 ust. 1 rozporządzenia KRI*	Regulacje dotyczące sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągnięcia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności SLA, mechanizmów kontroli i audytu. • Regulacje wewnętrzne opisujące wymagania w zakresie wdrażania systemów teleinformatycznych w urzędzie w zakresie: sposobu dostarczenia i instalacji systemu teleinformatycznego, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji, a także warunków i kryteriów odbioru. • Regulacje wewnętrzne opisujące sposób przeprowadzania zmian w systemach teleinformatycznych (w trakcie ich eksploatacji), w tym opis: sposobu zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany. • Regulacje wewnętrzne opisujące proces monitorowania systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanych wobec wzrostu ilości systemów teleinformatycznych, ilości przetwarzanych danych, ilości użytkowników poprzez podejmowanie działań zapobiegawczych. • Działania związane z wdrażaniem nowych systemów teleinformatycznych oraz wprowadzaniem zmian w systemach eksploatowanych. • Działania związane z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności. Działania zapobiegawcze będące wynikiem dostrzeżonych problemów podczas monitorowania ich pracy.	Dokumentacja SZBI zawiera regulacje wewnętrzne związane Z projektowaniem systemów teleinformatycznych, zostały zaprojektowane, wdrożone i eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk. Brak kadry /informatyka/ etatowej, prace projektowe i wykonawstwo realizują firmy zewnętrzne.	brak	S	Wicedyrektor	509619849
2.12	**Zabezpieczenia techniczno-organizacyjne dostępu do informacji**							

2.12.1	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zastosowanie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. Czy informacje są zabezpieczone w sposób uniemożliwiający nieuprawnionemu ich ujawnienie, modyfikacje, usunięcie lub zniszczenie? Czy ustalono zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych?	*§ 19 ust. 2 pkt 7 rozporządzenia KRI* *§ 19 ust. 2 pkt 9 rozporządzenia KRI* *§ 19 ust. 2 pkt 11 rozporządzenia KRI*	• Regulacje wewnętrzne w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych w tym plan postępowania z ryzykiem. • Regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie. • Działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu. • Działania związane z monitorowaniem ruchu osobowego w podmiocie. • Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia SZBI. • Działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. • Działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych zgodne z wynikami analizy	Dokumentacja SZBI zawiera regulacje wewnętrzne związane Z ochroną przetwarzanych informacji, brak komórki do realizacji i analiz i monitorowania pracy użytkowników (z wyjątkiem administratora dziennika elektronicznego, administratora strony www). Brak nadzoru mechanizmów lub niewykorzystywane mechanizmy kontroli zagrożeń w sieci Szkoły. Część infrastruktury opartej na „przetwarzaniu chmurowym" posiada zasady opracowane przez dostawców zewnętrznych.	brak	CS	Wicedyrektor	509619849

			ryzyka i planem postępowania z ryzykiem. • Działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie SZBI.					
2.13	**Zabezpieczenia techniczno-organizacyjne systemów informatycznych**							

2.13.1	Czy zapewniono odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegający w szczególności na: a) dbałości o aktualizację oprogramowania, b) minimalizowaniu ryzyka utraty informacji w wyniku awarii, c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją, d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, e) zapewnieniu bezpieczeństwa plików systemowych, f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.	*§ 19 ust. 2 pkt 12 rozporządzenia KRI*	• Regulacje wewnętrzne, w których ustalono zasady zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem. • Działania związane z aktualizacją oprogramowania oraz redukcją ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych poprzez wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. • Działania związane z minimalizowaniem ryzyka utraty informacji w wyniku awarii oraz ochroną przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnienie bezpieczeństwa plików systemowych poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych, w tym np.: dwustronnego bezprzerwowego zasilania, redundancji klimatyzacji, zastosowania klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia (ang. load balancing), monitorowania parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie, wyciek wody), zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów	Ustanowiono dokumentację i procedury SZBI lecz nadzór nad infrastrukturą opiera się o umowy z firmami zewnętrznymi (strona www, infrastruktura sieciowa Szkoły, brak serwerów i scentralizowanego zarzadzania na poziomie Active Directory). Stosowane oprogramowanie jest aktualizowane.	brak	CS	Wicedyrektor	509619849

			teleinformatycznych i sieci zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. • Działania związane z zastosowaniem mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa poprzez stosowanie zabezpieczeń kryptograficznych, np.: dla transmisji do urządzeń mobilnych, poczty elektronicznej a także podpisów kwalifikowanych do autoryzacji dokumentów zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. • Działania podejmowane w związku z dostrzeżeniem nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa. • Działania związane z kontrolą zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.				
2.13.2	Czy niezależnie od zapewnienia działań, o których mowa w § 19 ust. 2 rozporządzenia KRI, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne ustanowiono dodatkowe zabezpieczenia?	*§ 19 ust. 4 rozporządzenia KRI*	• Analiza ryzyka, plan postępowania z ryzykiem. Regulacje wewnętrzne stosowania zabezpieczeń dodatkowych.	Ustanowiono procedury w SZBI. Na podstawie przeprowadzonych analiz ryzyka brak konieczności ustanowienia dodatkowych zabezpieczeń.	brak	S	Wicedyrektor	509619849
2.14	**Rozliczalność działań w systemach teleinformatycznych**							
2.14.1	Czy w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa? Czy w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 19 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych,	*§ 20 ust. 2 rozporządzenia KRI* *§ 20 ust. 3 rozporządzenia KRI* *§ 20 ust. 4 rozporządzenia KRI*	• Regulacje wewnętrzne w których ustalono zasady prowadzenia i wykorzystania dzienników systemowych (logów) w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych. • Działania związane z zapewnieniem rozliczalności użytkowników z uprawnieniami administracyjnymi, działań związanych z konfiguracją systemu i zabezpieczeń, działań, gdy przetwarzanie danych podlega prawnej ochronie (np. dane osobowe). • Działania związane z zapewnieniem rozliczalności działań użytkowników lub obiektów systemowych a także rejestracji innych zdarzeń systemowych w zakresie wynikającym z analizy ryzyka. • Działania związane z regularnym przeglądaniem logów i ich analizą w celu	W toku przeprowadzania czynności audytowych stwierdzono ustanowienie mechanizmów wewnętrznych regulujących przechowywanie zapisów z dzienników systemów teleinformatycznych, brak jednak mechanizmów sieci hierarchicznej. W systemach teleinformatycznych dostęp odbywa się przez uprawnione osoby i procesy w ustalonym zakresie; Brak lokalnego serwera /Active Directory/ utrudnia analizę logów systemowych. Nie dokonuje się okresowych przeglądów sieci.	brak	N	Wicedyrektor	509619849

	2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny? Czy informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata?		identyfikacji działań niepożądanych. • Okres i sposób przechowywania dzienników systemowych.	Brak dokumentów audytów sieci informatycznej i oprogramowania i testów penetracyjnych.				
3	**Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych**							
3.1	Czy system teleinformatyczny spełnia wymagania Web Content Accessibility Guidelines (WCAG 2.1), z uwzględnieniem poziomu AA, określonym w załączniku do ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (t.j. Dz.U. z 2023 poz. 1440)	*Załącznik do ustawy z dnia 4 kwietnia 2019 r o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych*	• Sposób prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu.	Strona https://www.zsllesko.pl spełnia wymogi WCAG 2.1(AA) z dużą ilością błędów (powyżej 60). Strona BIP https://www.zsllesko.pl/bip spełnia wymogi WCAG 2.1(AA) z błędami (19). (Testowano oprogramowaniem Pomocnik WCAG 2.1 Installer). Strona posiada certyfikat SSL	brak	S	Wicedyrektor	509619849

Objaśnienia:

S – wymaganie spełnione,
N – wymaganie niespełnione, CS – wymaganie częściowo spełnione, ND – nie dotyczy.
Kolumna nr 7, 8 – osobę przygotowującą odpowiedź, posiadającą wiedzę źródłową w zakresie danego wymagania.

12.12.2024 r.

KIEROWNIK GOSPODARCZY
Zespołu Szkół Leśnych w Lesku
mgr Robert Pałka

.....
data i podpis audytora
jednostki

DYREKTOR
Zespołu Szkół Leśnych w Lesku
mgr Jadwiga Szylak

.....
data i podpis kierownika
12.12.2024