Cyberbezpieczeństwo w placówce oświatowej

Mapa kompetencji kadry zarządzającej placówkami oświatowymi

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
MAŁOPOLSKA

Mapa kompetencji

Publikacja współfinansowana ze środków Unii Europejskiej w ramach Krajowego Planu Odbudowy i Zwiększenia Odporności, inwestycja A3.1.1 Wsparcie rozwoju nowoczesnego kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie.

Przedsięwzięcie: Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych.

Członkowie zespołu badawczego

dr Bartłomiej Balsamski

dr hab. Magdalena Jelonek, prof. UEK

mgr Sylwia Kołdras

dr Piotr Kopyciński

mgr Marcin Kukiełka

mgr Magdalena Nalepa-Rybarska

mgr Wojciech Pelowski

mgr inż. Wojciech Sypek

mgr Izabela Władyka

mgr Cecylia Zięba

Rysunek na okładce został wygenerowany przy użyciu AI.

Kraków 2026

Niniejszy dokument umożliwia samodzielną ocenę stanu cyberbezpieczeństwa w placówce oświatowej. Weryfikacja polega na sprawdzeniu, czy realizowane są określone procedury przypisane do poszczególnych kategorii. Osiągnięcie poziomu minimalnego lub oczekiwanego wymaga spełnienia wszystkich wytycznych w danym obszarze. Z kolei niezrealizowane procedury bezpośrednio wskazują luki kompetencyjne, definiując tym samym rekomendowany zakres tematyki szkoleń. Należy zaznaczyć, że niniejsza samoocena obejmuje najważniejsze, lecz nie wszystkie aspekty cyberbezpieczeństwa.

Proces opracowania Mapy kompetencji z zakresu cyberbezpieczeństwa, adresowanej do kadry zarządzającej (KZ) ryzykiem w placówkach oświatowych, składał się z wielu etapów opisanych poniżej. Pracę rozpoczęto od przeglądu istniejących materiałów oraz zagadnień pomocnych przy tworzeniu mapy (etap Analiza dostępnych materiałów), które posłużyły jako podstawa teoretyczna do utworzenia dokumentu. Zdefiniowane zostały tam kluczowe zagadnienia, warte weryfikacji ich stanu faktycznego. Następnie opracowano pytania wykorzystane podczas przeprowadzonych mini-audytów mających na celu ocenę rzeczywistego stanu w placówkach oświatowych (etap Przeprowadzenie mini-audytów). Utworzone na potrzeby mini-audytów pytania zostały zagregowane w logiczne bloki tematyczne, rozszerzające zdefiniowane we wcześniejszych krokach standardy. Prace te doprowadziły do powstania następujących kategorii zagrożeń cyberbezpieczeństwa:

- zarządzanie cyberbezpieczeństwem,
- zarządzanie hasłami i uwierzytelnianiem,
- bezpieczeństwo komunikacji elektronicznej,
- ewidencja zasobów, monitorowanie i analiza zdarzeń,
- zarządzanie tożsamością i dostępem,
- kopie zapasowe i odtwarzanie danych,
- ochrona danych osobowych i prywatności,
- budowanie kultury bezpieczeństwa,
- przechowywanie, udostępnianie i ochrona danych,
- bezpieczeństwo urządzeń końcowych,
- bezpieczeństwo sieci i infrastruktury.

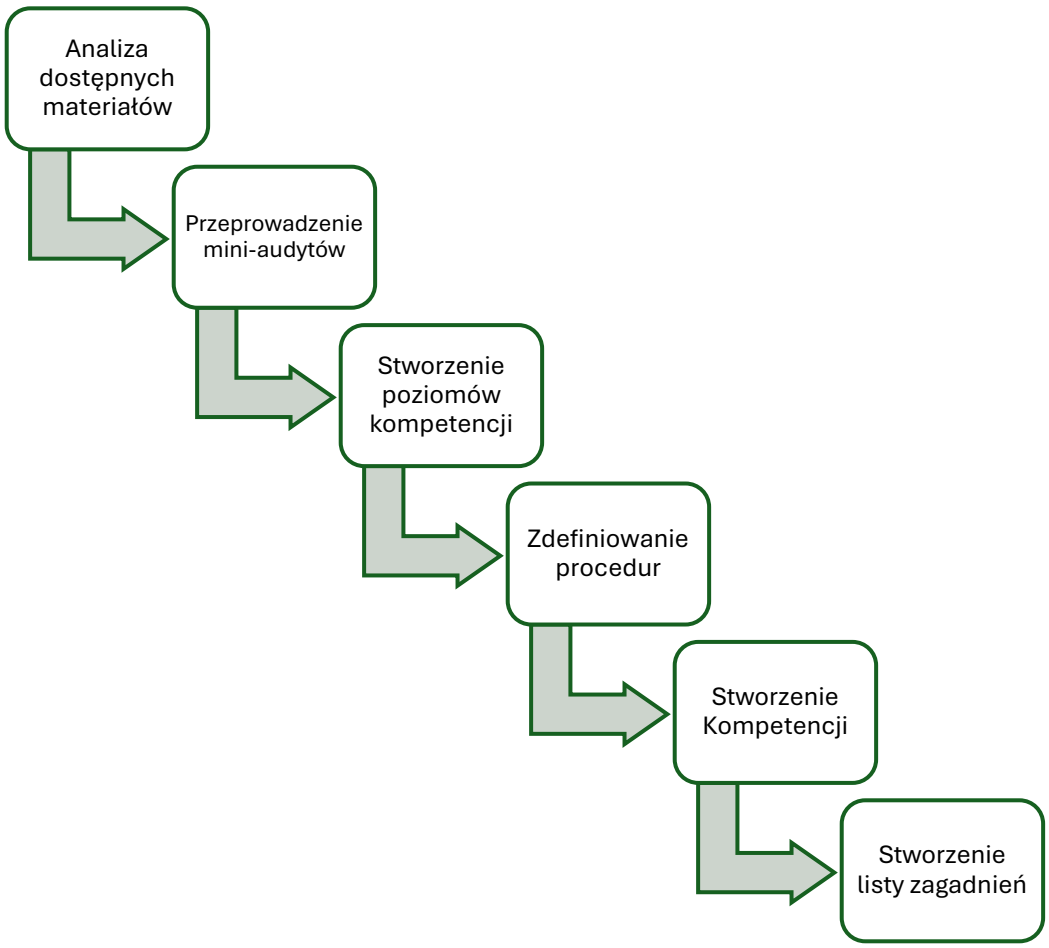
Podział ten stworzył fundament do dalszych prac, podczas których zostały określone rekomendowane poziomy (etap Stworzenie poziomów kompetencji). Dla każdej z kategorii zdefiniowano dwustopniową skalę oceny:

- Poziom Minimalny: określa niezbędną bazę – zestaw podstawowych działań zabezpieczających i organizacyjnych, które każda placówka musi bezwzględnie realizować, aby zapewnić elementarną ochronę danych i systemów.

- Poziom Oczekiwany: wskazuje bardziej zaawansowane procedury oraz dojrzałą kulturę organizacyjną, stanowiąc punkt docelowy dla optymalnego funkcjonowania szkoły.

Kolejny etap (etap Zdefiniowanie procedur) to działanie mające na celu przyporządkowanie dla każdego z poziomów, w obrębie wszystkich kategorii, określonych procedur operacyjnych. Utworzone w ten sposób procedury stanowiły podstawę do przełożenia ich na odpowiednie kompetencje Kadry Zarządzającej (etap Stworzenie Kompetencji). Transformacja ta opiera się na założeniu, że w obszarze cyberbezpieczeństwa kompetencje kadry zarządzającej wprost odnoszą się do rekomendowanych praktyk działania. Ostatnim etapem prac (etap Stworzenie listy zagadnień) było zdefiniowanie, na bazie opracowanych kompetencji i procedur, niezbędnych zagadnień szkoleniowych, w zakresie których placówka musi się doskonalić, aby osiągnąć poziom oczekiwany w poszczególnych kategoriach. Etapy zostały zilustrowane na rysunku 1.

Rysunek 1. Etapy stworzenia mapy kompetencji



Źródło: Opracowanie własne.

Kategoria	Poziom	Procedury	Kompetencje	Lista zagadnień
Zarządzanie cyberbezpieczeństwem	Minimalny	1. Organizacja cyklicznych szkoleń z zakresu cyberbezpieczeństwa dla nauczycieli.	1. Kadra zarządzająca (KZ) reaguje na incydenty bezpieczeństwa zgodnie z procedurami określonymi w polityce. [W, U, P]	• Główne założenia i zadania Polityki Cyberbezpieczeństwa • Procedury reagowania na incydenty oraz ścieżki ich zgłaszania
		2. Utrzymanie i aktualizacja Polityki Cyberbezpieczeństwa zawierającej instrukcje reagowania na incydenty.	2. KZ udostępnia politykę cyberbezpieczeństwa wewnątrz szkoły oraz aktywnie dba o jej aktualność. [W, P]	
			3. KZ organizuje i przeprowadza regularne szkolenia z zakresu cyberbezpieczeństwa. [U, P]	
	Oczekiwany	1. Formalne wyznaczenie (np. poprzez oddelegowanie) pracownika pełniącego rolę koordynatora ds. cyberbezpieczeństwa w placówce.	1. KZ zatrudnia lub wyznacza (oddelegowuje) konkretną osobę odpowiedzialną za codzienne, praktyczne egzekwowanie polityki. [W, P]	• Rola, obowiązki i narzędzia pracy koordynatora ds. cyberbezpieczeństwa. • Metodyka planowania i prowadzenia obowiązkowych szkoleń (programów świadomościowych) dla kadry i uczniów
		2. Wdrożenie kompleksowego programu szkoleń obejmującego kadrę pedagogiczną, administracyjną oraz uczniów.	2. KZ planuje i wdraża obowiązkowe szkolenia dedykowane nie tylko kadrze, ale również uczniom. [W, U, P]	
Zarządzanie hasłami i uwierzytelnianiem	Minimalny	1. Procedura obowiązkowego uwierzytelniania wieloskładnikowego (MFA) w kluczowych systemach.	1. KZ stosuje uwierzytelnianie wieloskładnikowe (MFA) w systemach. [W, U, P]	• Obsługa uwierzytelniania wieloskładnikowego (MFA). • Zasady tworzenia silnych haseł • Zasady bezpiecznego przechowywania haseł
		2. Procedura reagowania na incydenty wymuszająca natychmiastową, globalną zmianę haseł po podejrzeniu wycieku.	2. KZ systemowo wymusza stosowanie mechanizmów MFA dla wszystkich użytkowników. [U, P]	
		3. Bezwzględny zakaz zapisywania haseł we wbudowanych menedżerach przeglądarek internetowych.	3. KZ wykorzystuje wyłącznie unikalne hasła dla każdego używanego systemu. [W, P]	
		4. Wymóg tworzenia unikalnych haseł dla każdej usługi.	4. KZ bezzwłocznie wymusza systemową zmianę haseł na wszystkich użytkownikach w przypadku incydentu. [U, P]	
			5. KZ natychmiast zmienia hasła po powzięciu informacji o wycieku. [W, U, P]	
			6. KZ nie zapisuje haseł w przeglądarkach internetowych. [P]	
	Oczekiwany	1. Zapewnienie i wymóg korzystania z fizycznych kluczy sprzętowych (np. YubiKey) dla dostępów najwyższego ryzyka.	1. KZ aktywnie korzysta z menedżera haseł do ich bezpiecznego przechowywania. [W, U, P]	• Zastosowanie fizycznych kluczy sprzętowych • Konfiguracja i obsługa menedżera haseł
		2. Procedura bezpiecznego przechowywania zapasowych (backupowych) kluczy sprzętowych.	2. KZ stosuje fizyczne klucze sprzętowe (oraz dba o ich backup) do zabezpieczania dostępu. [W, U, P]	
		3. Wdrożenie scentralizowanego menedżera haseł dedykowanego wyłącznie do poświadczeń służbowych (oddzielonego od danych prywatnych).		

Kategoria	Poziom	Procedury	Kompetencje	Lista zagadnień
Bezpieczeństwo komunikacji elektronicznej	Minimalny	1. Prowadzenie służbowej komunikacji elektronicznej wyłącznie poprzez zatwierdzone kanały (e-dziennik, służbowy e-mail).	1. KZ stosuje w sprawach szkolnych wyłącznie oficjalne kanały komunikacji (np. służbowy e-mail). [W, P]	• Zasady bezpiecznej komunikacji mailowej • Zagrożenia w komunikacji mailowej – Identyfikacja phishingu • Procedury szyfrowania załączników zawierających dane wrażliwe. • Obsługa ministerialnych platform teleinformatycznych
		2. Zakaz przesyłania i przekierowywania danych szkolnych na prywatne skrzynki pocztowe.	2. KZ nie przekierowuje służbowej korespondencji na skrzynki prywatne. [P]	
		3. Zakaz korzystania z grupowych, współdzielonych (gdzie jedno hasło zna wiele osób) skrzynek pocztowych.	3. KZ eliminuje praktykę korzystania z jednych, współdzielonych skrzynek pocztowych przez wielu pracowników. [W, P]	
		4. Procedura obowiązkowego wykorzystywania pola ukrytej kopii (UDW/BCC) przy masowej wysyłce wiadomości do wielu odbiorców.	4. KZ bezwzględnie stosuje funkcję ukrytej kopii (UDW) przy masowej wysyłce korespondencji. [W, U, P]	
		5. Weryfikacji tożsamości nadawców wiadomości w celu minimalizowania ryzyka phishingu.	5. KZ aktywnie weryfikuje nadawców wiadomości przed podjęciem akcji (np. kliknięciem w link). [W, P]	
		6. Konieczność szyfrowania każdego załącznika zawierającego dane wrażliwe (np. RODO, dane finansowe).	6. KZ każdorazowo szyfruje załączniki zawierające dane wrażliwe (np. RODO, finanse). [W, U, P]	
		7. Stosowanie we wszystkich możliwych miejscach wskazanych przez ministerstwo systemów i platform teleinformatycznych (np. e-doręczenia) do oficjalnej wysyłki i obiegu dokumentów	7. KZ wdraża, utrzymuje i egzekwuje wykorzystanie oficjalnych narzędzi ministerialnych (np. e-doręczenia) w zewnętrznej korespondencji urzędowej placówki. [W, U, P]	
	Oczekiwany	1. „Separacja kanałów" – przesyłanie hasła do odszyfrowania załącznika innym kanałem niż sam plik (np. plik e-mailem, hasło SMS-em).	1. KZ przekazuje hasło do zaszyfrowanego załącznika alternatywnym, odseparowanym kanałem. [W, U, P]	• Zaawansowane procedury szyfrowania załączników zawierających dane wrażliwe.
		2. Uwierzytelnianie kluczowych dokumentów wewnętrznych i zewnętrznych za pomocą kwalifikowanego podpisu elektronicznego.	2. KZ stosuje kwalifikowany podpis elektroniczny do autoryzacji elektronicznego obiegu dokumentów. [W, U, P]	
		3. Zasada przydzielania zindywidualizowanych kont e-mail w zarejestrowanej domenie szkoły każdemu pracownikowi (np. imie.nazwisko@szkola.pl).	3. KZ zakłada i przydziela każdemu pracownikowi zindywidualizowany adres e-mail we własnej domenie szkoły. [W, U]	
Ewidencja zasobów, monitorowanie i analiza zdarzeń	Minimalny	1. Szkoła posiada scentralizowany rejestr używanego oprogramowania i posiadanych licencji.	1. KZ tworzy, prowadzi i na bieżąco aktualizuje centralny rejestr wszystkich posiadanych licencji oprogramowania. [W, U, P]	• Zasady prowadzenia rejestru licencji oprogramowania.
	Oczekiwany	1. Szkoła rejestruje aktywności użytkowników w kluczowych systemach szkolnych (e-mail, e-dziennik).	1. KZ konfiguruje używane systemy tak, aby generowały szczegółowe logi zdarzeń. [W, U]	• Podstawy monitorowania i analizy logów w celu wykrywania anomalii.
		2. Przypisanie odpowiedzialności wyznaczonemu pracownikowi za cykliczny przegląd logów systemowych pod kątem anomalii.	2. KZ wyznacza pracownika odpowiedzialnego za cykliczną analizę logów i reagowanie na anomalie. [W, P]	

Kategoria	Poziom	Procedury	Kompetencje	Lista zagadnień
Zarządzanie tożsamością i dostępem	Minimalny	1. Procedura natychmiastowego blokowania kont i odbierania uprawnień systemowych w dniu zakończenia współpracy z pracownikiem.	1. KZ niezwłocznie blokuje dostępy do systemów szkolnych pracownikom kończącym współpracę. [U, P]	• Zastosowanie zasady minimalnych uprawnień w pracy z danymi
		2. Wdrożenie zasady minimalnych uprawnień (np. nauczyciel ma dostęp tylko do danych swoich klas).	2. KZ ogranicza i przydziela dostęp do danych zgodnie z zasadą wiedzy niezbędnej. [W, U]	
	Oczekiwany	1. Wdrożenie mechanizmu Single Sign-On (SSO) do scentralizowanego zarządzania tożsamością.	1. KZ wdraża mechanizmy pojedynczego logowania (SSO) do zarządzania dostępem. [W, U]	• Metodyka przeprowadzania okresowych audytów kont i uprawnień pracowników.
		2. Procedura okresowych audytów aktywnych kont i uprawnień pracowników, przeprowadzana przez administratora.	2. KZ zleca i nadzoruje regularną weryfikację (audyt) przyznanych pracownikom uprawnień. [W, P]	
Przechowywanie, udostępnianie i ochrona danych	Minimalny	1. Zakaz przetwarzania szkolnych danych wrażliwych na prywatnych urządzeniach pracowników.	1. KZ egzekwuje przetwarzanie danych szkolnych wyłącznie na autoryzowanym sprzęcie służbowym. [P]	• Znajomość zasad separacji środowiska prywatnego od służbowego
		2. Ograniczenie wykorzystywania szkolnego sprzętu służbowego do celów prywatnych.	2. KZ zabrania wykorzystywania sprzętu szkolnego do celów prywatnych. [P]	
		3. Wdrożenie zabezpieczonej chmury jako podstawowego i preferowanego sposobu transferu plików między urządzeniami.	3. KZ wymusza bezpieczne przenoszenie plików między urządzeniami z użyciem chmury. [U, P]	
	Oczekiwany	1. Konfiguracja i utrzymanie dedykowanej, oficjalnej chmury szkolnej do zastosowań zawodowych.	1. KZ wdraża i utrzymuje oficjalną chmurę szkolną dedykowaną do pracy zawodowej. [W, U]	• Zasady szyfrowanie przenośnych nośników pamięci
		2. Obowiązek szyfrowania wszystkich przenośnych nośników pamięci (pendrive, dyski zewnętrzne) używanych w placówce.	2. KZ szyfruje wszelkie zewnętrzne nośniki danych (pendrive, dyski) dopuszczone do użytku. [W, U, P]	
		3. Procedura cyklicznego weryfikowania i cofania dostępów do udostępnionych zewnętrznie zasobów chmurowych.	3. KZ regularnie kontroluje i cofa zbędne udostępnienia plików w chmurze. [U, P]	
Kopie zapasowe i odtwarzanie danych	Minimalny	1. Automatyzacja tworzenia kopii zapasowych najważniejszych systemów szkolnych z odpowiednią częstotliwością.	1. KZ konfiguruje i utrzymuje automatyczne procesy tworzenia kopii zapasowych najważniejszych systemów wg reguły 3-2-1. [W, U]	• Zasady funkcjonowania zautomatyzowanego procesu tworzenia kopii zapasowych. • Praktyczne zastosowanie reguły 3-2-1 w tworzeniu kopii zapasowych. • Procedury testowego odtwarzania danych w celu weryfikacji backupów.
		2. Zastosowanie reguły backupu 3-2-1 (3 kopie, 2 różne nośniki, 1 kopia w innej lokalizacji).	2. KZ cyklicznie testuje poprawność backupów poprzez próby odtworzenia z nich danych. [U, P]	
		3. Procedura okresowego, testowego odtwarzania danych w celu weryfikacji integralności backupów.		
	Oczekiwany	1. Opracowanie i wdrożenie procedury tworzenia kopii zapasowych bezpośrednio ze stacji roboczych (komputerów) nauczycieli.	1. KZ opracowuje i wdraża procedurę regularnego tworzenia kopii zapasowych bezpośrednio ze stacji roboczych nauczycieli. [W, U]	• Procedury i narzędzia do tworzenia kopii zapasowych ze stacji roboczych nauczycieli. • Zasady prowadzenia oficjalnej dokumentacji tworzonych kopii zapasowych.
		2. Prowadzenie i aktualizacja oficjalnej dokumentacji architektury backupu (opis częstotliwości, zakresu i miejsc przechowywania).	2. KZ tworzy i aktualizuje formalną dokumentację architektury kopii zapasowych. [W, U]	

Kategoria	Poziom	Procedury	Kompetencje	Lista zagadnień
Ochrona danych osobowych	Minimalny	1. Wymóg zabezpieczania dostępu do profili na stacjach roboczych indywidualnym, silnym hasłem.	1. KZ zabezpiecza fizyczny i logiczny dostęp do stacji roboczych silnymi hasłami. [U, P]	• Zasady cyfrowej higieny
		2. Systemowa konfiguracja wymuszająca automatyczne blokowanie ekranu urządzenia po ustalonym czasie bezczynności.	2. KZ systemowo konfiguruje automatyczne blokowanie ekranów urządzeń po czasie bezczynności. [U]	
	Oczekiwany	1. Weryfikowanie zgód przed jakąkolwiek publikacją wizerunku ucznia/nauczyciela.	1. KZ zawsze pozyskuje i weryfikuje formalne zgody na wykorzystanie wizerunku przed jego publikacją. [W, P]	• Szkolenie z zasad RODO • Procedury prawne i techniczne pozyskiwania oraz weryfikacji zgód na publikację wizerunku.
Budowanie kultury bezpieczeństwa	Minimalny	1. Jasno zdefiniowana i łatwo dostępna ścieżka zgłaszania incydentów naruszenia bezpieczeństwa.	1. KZ opracowuje i jasno komunikuje procedurę zgłaszania incydentów naruszenia bezpieczeństwa. [W, U]	• Jasne ścieżki i procedury zgłaszania incydentów naruszenia bezpieczeństwa •
		2. Procedura obowiązkowego rejestrowania i analizowania wszystkich zaistniałych incydentów.	2. KZ skrupulatnie rejestruje i analizuje każdy zgłoszony przypadek. [U, P]	• Zasady rejestrowania i analizy zgłoszonych przypadków naruszeń
	Oczekiwany	1. Budowanie kultury braku oskarżeń.	1. KZ buduje kulturę zaufania (ang. „blame-free”), skupiając się na procesie naprawczym, a nie na karaniu pracowników, którzy niezwłocznie zgłosili własny błąd. [W, P]	• Budowanie przyjaznego środowiska pracy • Kultura zaufania „blame-free”
Bezpieczeństwo urządzeń końcowych	Minimalny	1. Szkoła posiada standardową konfigurację ograniczającą uprawnienia (odebranie uprawnień administratora lokalnego zwykłym użytkownikom).	1. KZ odbiera standardowym użytkownikom uprawnienia administracyjne na ich stacjach roboczych. [W, U]	• Znaczenie automatycznego instalowania aktualizacji systemowych
		2. Polityka wymuszająca automatyczne pobieranie i instalowanie aktualizacji systemowych.	2. KZ wymusza automatyczne instalowanie aktualizacji systemowych oraz poprawek bezpieczeństwa. [U]	
	Oczekiwany	1. Blokada możliwości samodzielnego instalowania dowolnego (nieautoryzowanego) oprogramowania przez użytkowników.	1. KZ technicznie blokuje możliwość instalacji niezatwierdzonego oprogramowania na sprzęcie szkolnym. [U]	• Znaczenie ograniczenia dostępu do stacji roboczych: blokady instalacji nieautoryzowanego oprogramowania
		2. Systemowa (lub fizyczna) blokada portów uniemożliwiająca podłączanie prywatnych, nieautoryzowanych nośników (np. pendrive’ów).	2. KZ systemowo blokuje możliwość podłączania prywatnych nośników pamięci (np. prywatne pendrive’y). [U]	
Bezpieczeństwo sieci i infrastruktury	Minimalny	1. Zabezpieczenie sieci bezprzewodowych (WiFi) silnymi protokołami szyfrowania i hasłami.	1. KZ zabezpiecza szkolną sieć bezprzewodową zgodnie z aktualnymi standardami szyfrowania. [W, U]	• Standardy szyfrowania szkolnych sieci bezprzewodowych WiFi • Fizyczne zabezpieczanie infrastruktury (szafy RACK, serwerownie)
		2. Restrykcyjny dostęp fizyczny do urządzeń sieciowych (zamykane na zamek szafy serwerowe / routery).	2. KZ fizycznie zabezpiecza urządzenia dostępowe (np. zamyka szafy RACK, serwerownie). [W, P]	
	Oczekiwany	1. Posiadanie odseparowanej sieci bezprzewodowej przeznaczonej wyłącznie dla gości.	1. KZ stosuje dedykowaną, izolowaną sieć WiFi przeznaczoną wyłącznie dla gości. [W, U]	• Podstawy segmentacji sieci lokalnej (VLAN)
		2. Wdrożenie segmentacji sieci lokalnej (VLAN) w celu oddzielenia ruchu i danych administracji, nauczycieli oraz uczniów.	2. KZ stosuje technicznie ograniczenia sieci (VLAN), oddzielając ruch administracji, nauczycieli oraz uczniów. [W, U]	

OŚWIADCZENIE O WYKORZYSTANIU NARZĘDZI SZTUCZNEJ INTELIGENCJI *(zgodnie z wytycznymi Zarządzenia Rektora Uniwersytetu Ekonomicznego w Krakowie z 24 lutego 2025 r. w sprawie zasad wykorzystania sztucznej inteligencji przy przygotowywaniu prac pisemnych)*

Narzędzie AI – Gemini (model językowy firmy Google) zostało zastosowane wyłącznie jako wsparcie asystujące, redakcyjne i analityczne na bazie materiałów źródłowych dostarczonych przez autora. Zakres wykorzystania AI obejmował:

1. **Strukturyzację i formatowanie dokumentu**: Przekształcenie list procedur w formalne, zorganizowane tabele przy tworzeniu „Mapy Kompetencji".
2. **Korektę językową i ujednolicenie stylu**: Przeformułowanie biernych opisów kompetencji na sformułowania w stronie czynnej, zorientowane na aktywne działanie.
3. **Kategoryzację i klasyfikację danych**: Wsparcie w przypisywaniu konkretnych działań technicznych i organizacyjnych do odpowiednich typów kompetencji.