PREZYDENT MIASTA KRAKOWA

OR-03.0003.150.2026

Pan
Bartłomiej Kocurek
Radny Miasta Krakowa

Odpowiadając na Pana interpelację w sprawie cyberbezpieczeństwa, przekazaną przez Pana Jakuba Koska, Przewodniczącego Rady Miasta Krakowa 26 lutego 2026 r., uprzejmie informuję.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii*, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80) została implementowana do polskiego porządku prawnego w drodze ustawy z dnia 23 stycznia 2026 r. *o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*. Ustawa ta została ogłoszona w Dzienniku Ustaw 2 marca 2026 r., poz. 252 i wejdzie w życie 3 kwietnia 2026 r. Nie oznacza to jednak, że Gmina Miejska Kraków nie czyni przygotowań do wdrożenia nowych regulacji. Już od zeszłego roku były podejmowane działania edukacyjne i zarządcze mające na celu przygotowanie jednostek organizacyjnych Gminy Miejskiej Kraków do nowego stanu prawnego.

I. Obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa

Ad 1.

Miasto realizuje obowiązek zarządzania bezpieczeństwem systemów informacyjnych w oparciu o formalnie przyjętą politykę bezpieczeństwa. Każda z jednostek organizacyjnych Gminy Miejskiej Kraków prowadzi dokumentację w tym obszarze.

Ad 2.

W okresie ostatnich 3 lat regularnie przeprowadzano audyty bezpieczeństwa systemów informacyjnych. Na przykład Centrum Audytu i Kontroli Analitycznej przeprowadziło następujące audyty:

Rok 2023

- 12 audytów zapewniających dotyczących procesu doskonalenia w obszarze bezpieczeństwa teleinformatycznego w Urzędzie Miasta Krakowa (IT) oraz 11 miejskich jednostkach organizacyjnych (Klimat-Energia-Gospodarka Wodna, Miejskie Centrum Obsługi Oświaty w Krakowie, Miejski Ośrodek Pomocy Społecznej w Krakowie, Straż Miejska Miasta Krakowa, Zarząd Budynków Komunalnych w Krakowie, Zarząd Cmentarzy Komunalnych w Krakowie, Zarząd Dróg Miasta Krakowa, Zarząd Inwestycji Miejskich w Krakowie, Zarząd Infrastruktury Sportowej w Krakowie, Zarząd Transportu Publicznego w Krakowie, Zarząd Zieleni Miejskiej w Krakowie),
- 1 audyt zapewniający dotyczący zabezpieczeń systemu IT, obejmujący elementy testu penetracyjnego (w Zarządzie Dróg Miasta Krakowa).

Rok 2024

- 5 audytów zapewniających dotyczących zarządzania oprogramowaniem i bezpieczeństwa domeny AD w 5 miejskich jednostkach organizacyjnych (ZZM, MOPS, MCOO, ZIS i ST),
- 3 audyty zapewniające dotyczące procesów merytorycznych, w ramach których oceniano bezpieczeństwo systemów informatycznych wspierających te procesy w Urzędzie Miasta Krakowa i miejskich jednostkach organizacyjnych (Krakowskie Centrum Kontaktu, Wydział Skarbu Miasta, ZIM).

Rok 2025

- 1 audyt zapewniający dotyczący procesu zarządzania transportem publicznym, w ramach którego oceniano bezpieczeństwo systemów informatycznych wspierających ten proces (w ZTP),
- 7 audytów zapewniających dotyczących zarządzania oprogramowaniem, bezpieczeństwa systemów informatycznych i wdrożenia ISO 27001 w miejskich jednostkach organizacyjnych (ZIM, ZIW, Miejskie Centrum Opieki w Krakowie, Szpital im. Gabriela Narutowicza, Szpital im. Stefana Żeromskiego, ZIS, ZBK);
- 1 audyt doradczy dotyczący zarządzania cyberbezpieczeństwem na poziomie Gminy Miejskiej Kraków (UMK i miejskie jednostki organizacyjne).

Ponadto w Urzędzie Miasta Krakowa, w związku z funkcjonującym Systemem Zarządzania Bezpieczeństwem Informacji według wymagań normy ISO 27001, wykonywane są zaplanowane audyty bezpieczeństwa informacji.

Ad 3.

W Gminie Miejskiej Kraków podmiotami świadczącymi usługi kluczowe, zgodnie z załącznikiem nr 1 do ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* są następujące podmioty:

- Miejskie Przedsiębiorstwo Energetyki Cieplnej SA,
- Wodociągi Miasta Krakowa SA,
- Szpital Miejski Specjalistyczny im. Gabriela Narutowicza,
- Szpital Specjalistyczny im. Stefana Żeromskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej,
- Miejskie Centrum Opieki dla Osób Starszych, Przewlekle Niepełnosprawnych oraz Niesamodzielnych w Krakowie.

II. Zarządzanie ryzykiem i testowanie zabezpieczeń

Ad 1.

Wszystkie portale zewnętrzne podlegające Centrum Obsługi Informatycznej UMK są poddawane systematycznym testom penetracyjnym w cyklu ciągłym. Stanowi to realizację obowiązku monitorowania systemu informacyjnego.

Ad 2.

Miasto posiada i realizuje formalny proces zarządzania podatnościami.

Ad 3 i 5 .

Ze względu na bezpieczeństwo systemów IT, szczegółowe dane statystyczne oraz informacje o aktualnie otwartych podatnościach nie mogą zostać udostępnione. Zgodnie z art. 38 ustawy *o krajowym systemie cyberbezpieczeństwa* nie udostępnia się informacji, jeżeli ich ujawnienie naruszyłoby ochronę interesu publicznego w odniesieniu do bezpieczeństwa lub porządku publicznego. Ponadto zgodnie z ww. ustawą, informacje o podatnościach i ryzyku wystąpienia incydentów podlegają szczególnej ochronie. Ujawnienie precyzyjnej mapy podatności mogłoby zostać wykorzystane do przeprowadzenia prób ataków na infrastrukturę miejską.

Ad 4.

Podatności o statusie High i Critical usuwane są niezwłocznie po ich zidentyfikowaniu, co jest zgodne z obowiązkiem niezwłocznego podejmowania działań naprawczych.

III. Przygotowanie do wdrożenia dyrektywy NIS 2

Ad 1.

W ramach przygotowania do wdrożenia postanowień dyrektywy NIS 2 przeprowadzono analizę typu gap analysis w odniesieniu do wymogów ustawy *o krajowym systemie cyberbezpieczeństwa*.

Ad 2.

Opracowanie planu obejmującego Miasto i spółki komunalne jest aktualnie w toku. Należy podkreślić, że zmienione przepisy wprowadzają okres dostosowawczy, podczas którego kolejne wymagania będą musiały być spełniane. Jednostki organizacyjne Gminy Miejskiej Kraków będą dostosowywać swoje działania do nowych regulacji zgodnie z przepisami prawa.

Ad 3.

Władze Miasta są świadome obowiązków wynikających z nowej regulacji, w szczególności odpowiedzialności za wykonywanie obowiązków w zakresie cyberbezpieczeństwa, w szczególności zawartych w art. 8c-8e i art. 73a ustawy *o krajowym systemie cyberbezpieczeństwa*.

Ad 4.

Proces szacowania ryzyka w kontekście nowych obowiązków jest realizowany równolegle z wdrażaniem nowych przepisów.

IV. Procedura ujawniania podatności

Ad 1.

Miasto priorytetyzuje sformalizowane i kontraktowe metody badania bezpieczeństwa (np. audyty zewnętrzne i testy penetracyjne) nad modelami otwartymi typu bug bounty.

Ad 2.

Obecnie funkcjonuje formalna wewnętrzna procedura zgłaszania podatności, jednak nie utworzono dedykowanego kanału dla niezależnych badaczy zewnętrznych.

Ad 3.

Nie przewiduje się wdrażania programów typu bug bounty.

Ad 4.

W okresie ostatnich 3 lat nie odnotowano zgłoszeń incydentów ani nieprawidłowości od niezależnych badaczy.

z up. PREZYDENTA MIASTA

Łukasz Sęk
Zastępca Prezydenta Miasta Krakowa

Signed by / Podpisano przez:

Łukasz Bartłomiej Sęk
Gmina Miejska Kraków - Urząd Miasta Krakowa

Date / Data: 2026-03-12 15:15

Otrzymują:
1. Adresat
2. Wydział Organizacji i Nadzoru (OR-13)
3. Centrum Obsługi Informatycznej
4. Centrum Audytu i Kontroli Analitycznej
5. Biuro Nadzoru Właścicielskiego
6. Pełnomocnik PMK ds. Ochrony Informacji Niejawnych
7. Biuletyn Informacji Publicznej
8. aa