ZARZĄDZENIE Nr 260/2026

PREZYDENTA MIASTA WŁOCŁAWEK

z dnia 26 maja 2026 r.

w sprawie powołania struktur odpowiedzialnych za cyberbezpieczeństwo w Urzędzie Miasta Włocławek

Na podstawie art. 31 oraz art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r., poz. 1153 i 1436 oraz z 2026 r., poz. 252.) w związku z art. 8e i art. 14 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r., poz. 20 i 252),

zarządza się, co następuje:

§ 1. Powołuje się Panią Lidię Walczak na Pełnomocnika do Spraw Cyberbezpieczeństwa w Urzędzie Miasta Włocławek, zwanym dalej „Pełnomocnikiem".

§ 2. Do podstawowych zadań Pełnomocnika należy koordynowanie i nadzorowanie działań związanych z bezpieczeństwem informacji w Urzędzie Miasta Włocławek, zwany dalej Urzędem, w szczególności:

1) cykliczny przegląd i aktualizacja dokumentacji dotyczącej cyberbezpieczeństwa na podstawie informacji przekazywanych przez kierowników komórek organizacyjnych Urzędu;

2) koordynacja procesu analizy ryzyka w zakresie cyberbezpieczeństwa zgodnie z wewnętrznymi regulacjami, w tym nadzorowanie i koordynowanie wykonania analizy oraz przedstawianie jej wyników Prezydentowi Miasta;

3) koordynacja procesu zarządzania ciągłością działania zgodnie z wewnętrznymi regulacjami.

4) inicjowanie działań podnoszących świadomość pracowników Urzędu w zakresie zagrożeń dotyczących cyberbezpieczeństwa;

5) monitorowanie incydentów z zakresu cyberbezpieczeństwa oraz nadzór nad ich zgłaszaniem i analizą;

6) organizowanie i nadzorowanie okresowych audytów zewnętrznych z zakresu cyberbezpieczeństwa oraz koordynowanie przeprowadzenia zewnętrznego audytu bezpieczeństwa systemu informacyjnego nakazanego, w drodze decyzji, przez organ właściwy do spraw cyberbezpieczeństwa;

7) przedkładanie Prezydentowi Miasta okresowych raportów dotyczących stanu zagrożeń w sferze cyberbezpieczeństwa w Urzędzie Miasta oraz wyników przeglądów w tym zakresie;

8) bieżąca współpraca z Inspektorem Ochrony Danych (IOD) oraz Administratorami Systemów Informatycznych (ASI) w zakresie zapewnienia spójności podejmowanych działań ochronnych.

§ 3. Pełnomocnik zapewnia prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.

§ 4. Pełnomocnik koordynuje proces wdrażania, monitorowania i dostosowania odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, prawdopodobieństwo wystąpienia incydentów oraz skutki społeczne i gospodarcze, w szczególności:

1) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym, przy współudziale komórki organizacyjnej Urzędu właściwej w sprawach informatycznych, testowanie systemu informacyjnego;
2) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrolę dostępu;
3) bezpieczeństwo zasobów ludzkich;
4) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, służących do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a Urzędem;
5) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych;
6) edukację z zakresu cyberbezpieczeństwa dla pracowników Urzędu;
7) podstawowe zasady cyberhigieny;
8) polityki i procedury stosowania kryptografii, w tym w stosowanych przypadkach szyfrowania;
9) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz w warunkach wewnętrznych Urzędu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach;
10) polityki kontroli dostępu.

§ 5. Do zadań Pełnomocnika należy zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usług.

§ 6. Pełnomocnik odpowiada za koordynację zarządzania incydentami oraz stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usług.

§ 7. Pełnomocnik stosuje i na bieżąco aktualizuje, w porozumieniu z komórką organizacyjną Urzędu właściwą do spraw informatycznych, dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usług.

§ 8. Pełnomocnik klasyfikuje incydent jako poważny na podstawie progów uznania incydentu za poważny, podejmuje decyzję o zgłoszeniu wczesnego ostrzeżenia o incydencie poważnym oraz zleca zgłoszenie incydentu poważnego osobom wyznaczonym do kontaktu z właściwym Zespołem Reagowania na Incydenty

Bezpieczeństwa Komputerowego, zwanym dalej CSIRT, zgodnie z procedurą postępowania z incydentami, stanowiącą załącznik nr 11 do Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Przekazuje, na wniosek właściwego CSIRT, sprawozdanie okresowe z obsługi incydentu poważnego, a także przekazuje właściwemu CSIRT sprawozdanie końcowe z obsługi incydentu poważnego oraz na bieżąco współdziała z właściwym CSIRT podczas obsługi incydentu poważnego i incydentu krytycznego, przekazując, za pośrednictwem osób wyznaczonych do kontaktu, niezbędne dane.

§ 9. Pełnomocnik koordynuje całość zadań związanych z usuwaniem podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

§ 10. W przypadku zaistnienia poważnego cyberzagrożenia Pełnomocnik, za pośrednictwem komórki organizacyjnej Urzędu właściwej w sprawach informatycznych, informuje użytkowników swoich usług, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć. Informuje także tych użytkowników o samym poważnym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych. Obowiązek udzielania informacji użytkownikom swoich usług spoczywa na Pełnomocniku w przypadku incydentu poważnego, jeżeli ma on niekorzystny wpływ na świadczenie tych usług.

§ 11. Zobowiązuje się kierowników komórek organizacyjnych Urzędu Miasta Włocławek oraz wszystkich pracowników do ścisłej współpracy z Pełnomocnikiem oraz udzielania mu niezbędnych informacji i dokumentów koniecznych do prawidłowej realizacji wykonywanych przez niego zadań.

§ 12. Wykonanie zarządzenia powierza się Dyrektorowi Wydziału Kontroli.

§ 13. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Miasta.

§ 14. Zarządzenie wchodzi w życie z dniem 1 czerwca 2026 r.

PREZYDENT MIASTA
Krzysztof Kukucki

Sprawdzono pod względem legislacyjnym
RADCA PRAWNY
mgr Anna Kaniewska
Tr/W/-186
25.05.2026r

UZASADNIENIE

Projekt zarządzenia stanowi wykonanie regulacji zawartych w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, które przesądzają o konieczności powołania w Urzędzie Miasta wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo. W świetle powyższych przepisów przyjęto konwencje powołania pełnomocnika ds. cyberbezpieczeństwa, który podlegał będzie bezpośrednio Prezydentowi Miasta, a jego zakres odpowiedzialności i obowiązków uregulowany zostanie w niniejszym zarządzeniu.

SEKRETARZ MIASTA
Krzysztof Czerwiński

KIEROWNIK REFERATU
Jacek Wałdoch