ZAB.120.37.2026

ZARZĄDZENIE NR 37/2026
STAROSTY WŁOCŁAWSKIEGO

z dnia 20 lipca 2026 r.

w sprawie powołania struktur odpowiedzialnych za cyberbezpieczeństwo w Starostwie Powiatowym we Włocławku

Na podstawie art. 34 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie powiatowym (Dz. U. z 2025 r., poz. 1684 oraz z 2026 r., poz. 252 i poz. 912) w związku z art. 14 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r., poz. 20, poz. 252 i poz. 815), zarządza się, co następuje:

§ 1. Powołuje się Pana Piotra Komorowskiego na Pełnomocnika do Spraw Cyberbezpieczeństwa w Starostwie Powiatowym we Włocławku , zwanym dalej „Pełnomocnikiem".

§ 2. Do podstawowych zadań Pełnomocnika należy koordynowanie i nadzorowanie działań związanych z bezpieczeństwem informacji w Starostwie Powiatowym we Włocławku, zwany dalej starostwem, w szczególności:

1) cykliczny przegląd i aktualizacja dokumentacji dotyczącej cyberbezpieczeństwa na podstawie informacji przekazywanych przez kierowników komórek organizacyjnych starostwa;
2) koordynacja procesu analizy ryzyka w zakresie cyberbezpieczeństwa zgodnie z wewnętrznymi regulacjami, w tym nadzorowanie i koordynowanie wykonania analizy oraz przedstawianie jej wyników Staroście Włocławskiemu;
3) koordynacja procesu zarządzania ciągłością działania zgodnie z wewnętrznymi regulacjami;
4) inicjowanie działań podnoszących świadomość pracowników starostwa 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 Staroście Włocławskiemu okresowych raportów dotyczących stanu zagrożeń w sferze cyberbezpieczeństwa w starostwie 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 starostwa 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 starostwem;

5) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych;

6) edukację z zakresu cyberbezpieczeństwa dla pracowników starostwa;

7) podstawowe zasady cyberhigieny;

8) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz w warunkach wewnętrznych starostwa, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach; 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 starostwa 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,określoną w Systemie 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 starostwa 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 starostwa 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 Naczelnikowi Wydziału Zarządzania, Administracji i Bezpieczeństwa.

§ 13. Zarządzenie wchodzi w życie z dniem 20 lipca 2026 r.

Uzasadnienie

Zarządzenia stanowi wykonanie przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, które nakładają na podmioty publiczne obowiązek zapewnienia odpowiedniej organizacji systemu zarządzania cyberbezpieczeństwem, w tym wyznaczenia osób odpowiedzialnych za realizację zadań w tym zakresie.

Powołanie Pełnomocnika pozwoli na wyodrębnienie funkcji odpowiedzialnej za koordynację działań w obszarze cyberbezpieczeństwa, zapewni właściwy nadzór nad realizacją obowiązków ustawowych oraz usprawni proces planowania i wdrażania środków organizacyjnych i technicznych służących ochronie systemów teleinformatycznych Starostwa Powiatowego we Włocławku.

Przyjęcie zarządzenia przyczyni się do uporządkowania struktury organizacyjnej odpowiedzialnej za cyberbezpieczeństwo, usprawnienia obiegu informacji dotyczących zagrożeń i incydentów oraz zwiększenia odporności Starostwa Powiatowego we Włocławku na zagrożenia cybernetyczne. Wprowadzenie funkcji Pełnomocnika ds. Cyberbezpieczeństwa stanowi również element budowania spójnego systemu zarządzania cyberbezpieczeństwem, zgodnego z obowiązującymi przepisami prawa oraz dobrymi praktykami w zakresie ochrony informacji i systemów teleinformatycznych.

Mając na uwadze powyższe, wydanie niniejszego zarządzenia jest uzasadnione i celowe.