

**ZARZĄDZENIE NR 150/2025
BURMISTRZA GMINY I MIASTA WĘGLINIEC
z dnia 31.12. 2025r.**

w sprawie powołania Zespołu ds. Cyberbezpieczeństwa w Urzędzie Gminy i Miasta w Węglińcu

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153 z późn. zm.), art. 21 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.), w związku z dyrektywą (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS2) oraz przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług w zakresie funkcjonowania Krajowego Systemu e-Faktur (KSeF), mając na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa sieci i systemów informatycznych Urzędu Gminy i Miasta Węglińiec, zarządzam, co następuje:

§ 1

1. Powołuję Zespół ds. Cyberbezpieczeństwa w Urzędzie Gminy i Miasta w Węglińcu, zwany dalej „Zespołem”.
2. Zespół jest ciałem doradczo-koordynującym Burmistrza Gminy i Miasta Węglińiec w obszarze bezpieczeństwa informacji oraz bezpieczeństwa sieci i systemów informatycznych, w szczególności w zakresie spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa, dyrektywy NIS2 oraz bezpiecznego korzystania z Krajowego Systemu e-Faktur (KSeF).
3. Zespół działa na terenie Urzędu Gminy i Miasta w Węglińcu, z siedzibą przy ul. Sikorskiego 3, 59-940 Węglińiec.

§ 2

1. W skład Zespołu wchodzi w szczególności:

- 1) Przewodniczący Zespołu – Marcin Papla
- 2) Zastępca Przewodniczącego – Tomasz Ferens
- 3) Członkowie Zespołu

- a. Anna Ząbkowska
- b. Agata Adamczyk
- c. Beata Bogacz
- d. Barbara Czapiewska
- e. Irena Pawłowska
- f. Monika Puzon
- g. Marek Jeziorny

2. W pracach Zespołu mogą brać udział, z głosem doradczym, inne osoby zaproszone przez Przewodniczącego Zespołu.

§ 3

1. Do zadań Zespołu należy w szczególności:

- 1) koordynowanie działań Urzędu w zakresie zapewnienia bezpieczeństwa informacji oraz bezpieczeństwa sieci i systemów informatycznych, w tym systemów przetwarzających dane osobowe i dane finansowe;
- 2) identyfikacja, analiza i ocena ryzyka dla bezpieczeństwa sieci i systemów informatycznych Urzędu oraz przedstawianie Burmistrzowi propozycji dotyczących akceptacji, ograniczenia lub przeniesienia zidentyfikowanych ryzyk;
- 3) inicjowanie i opiniowanie wdrażania środków technicznych, organizacyjnych i proceduralnych służących ograniczaniu ryzyka, w szczególności w zakresie kontroli dostępu, uwierzytelniania, szyfrowania, tworzenia kopii zapasowych, aktualizacji oprogramowania oraz segmentacji sieci;
- 4) opracowywanie, aktualizacja oraz monitorowanie stosowania wewnętrznych procedur i polityk cyberbezpieczeństwa, w tym planów reagowania na incydenty oraz planu ciągłości działania w obszarze ICT;
- 5) współdziałanie z wyznaczoną osobą lub osobami odpowiedzialnymi za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (CSIRT NASK/MON/GOV), w tym przygotowywanie materiałów do zgłaszania incydentów oraz prowadzenie rejestru incydentów i podatności;
- 6) zapewnienie warunków organizacyjnych do wywiązywania się przez Urząd z obowiązków w zakresie zgłaszania i obsługi incydentów, w szczególności incydentów poważnych, zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa;
- 7) przygotowywanie rekomendacji i propozycji rozwiązań zmierzających do dostosowania Urzędu do wymogów wynikających z dyrektywy NIS2 oraz jej krajowej implementacji, w tym w obszarze zarządzania ryzykiem, ciągłości działania, bezpieczeństwa łańcucha dostaw oraz nadzoru kierownictwa nad cyberbezpieczeństwem;
- 8) identyfikacja systemów i usług Urzędu mogących zostać objętych zakresem przepisów implementujących dyrektywę NIS2 oraz przygotowywanie propozycji zmian strukturalnych i proceduralnych związanych z wyznaczeniem podmiotu kluczowego lub podmiotu ważnego;
- 9) opiniowanie projektów umów oraz zamówień dotyczących systemów informatycznych, usług chmurowych oraz usług serwisowych pod kątem wymogów cyberbezpieczeństwa i ochrony danych, w tym wymogów NIS2;
- 10) bieżące monitorowanie zmian przepisów prawa oraz wytycznych organów właściwych w zakresie cyberbezpieczeństwa, KSeF i ochrony danych, a także rekomendowanie niezbędnych aktualizacji dokumentacji wewnętrznej Urzędu;

2. W zakresie Krajowego Systemu e-Faktur (KSeF) do zadań Zespołu należy ponadto:

- 1) współpraca z komórką finansowo-księgową oraz informatyczną w zakresie bezpiecznego podłączenia i utrzymania integracji systemów finansowo-księgowych Urzędu z KSeF;
- 2) opiniowanie rozwiązań technicznych i organizacyjnych dotyczących uwierzytelniania oraz autoryzacji użytkowników KSeF, w tym zasad nadawania, zmiany i odbierania uprawnień oraz obsługi tokenów, certyfikatów i innych środków identyfikacji;
- 3) opracowanie i aktualizacja procedur wewnętrznych dotyczących obiegu, akceptacji i archiwizacji faktur ustrukturyzowanych, z uwzględnieniem wymagań w zakresie ochrony danych i cyberbezpieczeństwa;

4) określenie zasad tworzenia i przechowywania kopii zapasowych dokumentów oraz logów związanych z funkcjonowaniem KSeF w Urzędzie, a także zasad odtwarzania danych po incydencie;

5) definiowanie i opiniowanie wymogów bezpieczeństwa przy wyborze zewnętrznych dostawców systemów i usług informatycznych wykorzystywanych do obsługi KSeF w Urzędzie;

6) monitorowanie komunikatów Ministerstwa Finansów oraz Krajowej Administracji Skarbowej w zakresie zmian funkcjonowania KSeF oraz rekomendowanie dostosowania procedur Urzędu do aktualnych wymagań.

3. W zakresie podnoszenia świadomości i kompetencji pracowników do zadań Zespołu należy w szczególności:

1) opracowywanie i koordynowanie realizacji rocznych planów szkoleń z zakresu cyberbezpieczeństwa, w tym dotyczących bezpiecznego korzystania z systemów informatycznych Urzędu oraz KSeF;

2) przygotowywanie materiałów informacyjnych oraz zaleceń dla pracowników w zakresie bezpiecznego przetwarzania danych, ochrony haseł, identyfikacji prób phishingu oraz reagowania na podejrzane zdarzenia;

3) inicjowanie i prowadzenie działań podnoszących kulturę bezpieczeństwa informacji w Urzędzie, w tym okresowych kampanii informacyjnych i testów socjotechnicznych;

4) przedstawianie Burmistrzowi okresowych sprawozdań z realizacji działań szkoleniowych i świadomościowych.

§ 4

1. Zespół realizuje swoje zadania na podstawie rocznego planu pracy, zatwierdzanego przez Burmistrza Gminy i Miasta Węglińiec.

2. Posiedzenia Zespołu zwołuje Przewodniczący z własnej inicjatywy, na wniosek Burmistrza lub na wniosek co najmniej dwóch członków Zespołu, nie rzadziej niż raz na kwartał.

3. Z posiedzeń Zespołu sporządza się protokół, który zawiera w szczególności listę uczestników, porządek obrad, omówione zagadnienia oraz podjęte ustalenia i rekomendacje.

4. Zespół może podejmować ustalenia w trybie obiegowym, z wykorzystaniem środków komunikacji elektronicznej, w szczególności poczty elektronicznej oraz systemów pracy zdalnej, co dokumentuje się w formie notatki lub protokołu obiegowego.

5. Przewodniczący Zespołu przedstawia Burmistrzowi co najmniej raz w roku sprawozdanie z realizacji zadań Zespołu, w tym informację o stanie bezpieczeństwa sieci i systemów informatycznych Urzędu, istotnych incydentach oraz zrealizowanych działaniach naprawczych i zapobiegawczych.

§ 5

Wykonanie zarządzenia powierza się Sekretarzowi Gminy i Miasta Węglińiec.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz
Gminy i Miasta Węglińiec
Mariusz Węczorek

