Zarządzenie nr 59/XVI R/2026

Rektora Uniwersytetu Medycznego we Wrocławiu

z dnia 28 kwietnia 2026 r.

w sprawie powołania Zespołu ds. cyberbezpieczeństwa w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu

Na podstawie art. 23 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 r., poz. 1571 ze zm.) zarządzam, co następuje:

§ 1

1. Powołuje się Zespół do spraw cyberbezpieczeństwa w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, zwany dalej Zespołem, w składzie:
    1) Wojciech Mech - Kierownik Centrum Informatycznego - Koordynator Zespołu,
    2) Piotr Tomaszewski – Kierownik Sekcji Sieci i Systemów Informatycznych,
    3) Bartosz Bielak – Kierownik Sekcji Serwisu Sprzętu i Wsparcia Użytkowników,
    4) Krzysztof Hebzda – Główny specjalista – administrator sieci,
    5) Tomasz Sołtysiński – Starszy specjalista ds. administrowania systemami,
    6) Piotr Gil – Webmaster.
2. Posiedzenia Zespołu zwołuje Koordynator.
3. W posiedzeniach Zespołu mogą uczestniczyć inne osoby wskazane przez Koordynatora.

§ 2

1. Celem działania Zespołu jest zapewnienie bieżącego monitorowania zagrożeń oraz skutecznego reagowania na incydenty bezpieczeństwa w systemach i infrastrukturze informatycznej Uczelni.
2. Zespół odpowiada za identyfikację podatności, ograniczanie ryzyka technicznego oraz wsparcie jednostek organizacyjnych w zakresie zapobiegania i minimalizowania skutków zdarzeń z obszaru cyberbezpieczeństwa.

§ 3

Do zadań zespołu należą:

1) Monitorowanie i analiza zagrożeń, polegające w szczególności na:
    a) monitorowaniu zagrożeń w cyberprzestrzeni w kontekście systemów, usług i infrastruktury Uczelni;
    b) analizie bieżących incydentów i trendów zagrożeń mających wpływ na bezpieczeństwo Uczelni;
    c) identyfikacji potencjalnych zagrożeń dla pracowników, studentów oraz systemów informatycznych.
2) Zarządzanie incydentami bezpieczeństwa, polegające w szczególności na:
    a) przyjmowaniu, rejestrowaniu i klasyfikacji zgłoszeń incydentów bezpieczeństwa;
    b) obsłudze incydentów takich jak:

- ataki hakerskie,
- infekcje złośliwym oprogramowaniem,
- naruszenia poufności, integralności lub dostępności danych;

c) koordynacji działań technicznych związanych z obsługą incydentu;

d) eskalacji incydentów do właściwych jednostek i osób decyzyjnych;

e) wsparciu technicznym jednostek Uczelni w trakcie trwania incydentu.

3) Analiza podatności i ocena ryzyka technicznego, polegające w szczególności na:

a) identyfikacji luk bezpieczeństwa w systemach informatycznych i infrastrukturze;

b) przeprowadzaniu technicznych ocen ryzyka dla systemów i usług;

c) analizie konfiguracji systemów pod kątem bezpieczeństwa;

d) rekomendowaniu działań ograniczających ryzyko techniczne.

4) Reagowanie i ograniczenie skutków zagrożeń, polegające w szczególności na:

a) podejmowaniu działań technicznych mających na celu ograniczenie skutków incydentów;

b) wsparciu w przywracaniu ciągłości działania systemów po incydencie;

c) wdrażaniu środków zapobiegawczych wynikających z analizy incydentów;

d) współpracy z administratorami systemów i sieci w zakresie zabezpieczania środowisk.

5) Współpraca wewnętrzna i zewnętrzna, polegająca w szczególności na:

a) współpracy z zespołami IT i administratorami systemów Uczelni w zakresie bezpieczeństwa;

b) współdziałaniu z innymi jednostkami organizacyjnymi w przypadku wystąpienia incydentów.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Uniwersytet Medyczny we Wrocławiu

REKTOR

prof. dr hab. Piotr Ponikowski

Otrzymują:
według rozdzielnika
UK