

Zarządzenie nr 139/XVI R/ 2025
Rektora Uniwersytetu Medycznego we Wrocławiu
z dnia 26 sierpnia 2025 r.

zmieniające zarządzenie w sprawie wprowadzenia Polityki ochrony danych osobowych Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, Instrukcji zarządzania siecią i systemami informatycznymi w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Regulaminu monitoringu wizyjnego w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Procedury fizycznego dostępu do pomieszczeń oraz dokumentów zawierających dane osobowe przechowywanych w wersji papierowej w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu oraz Procedury ochrony danych osobowych w badaniach naukowych prowadzonych 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

W Instrukcji zarządzania siecią i systemami informatycznymi Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, stanowiącej załącznik nr 2 do zarządzenia nr 93/XV R/2018 Rektora Uniwersytetu Medycznego we Wrocławiu z dnia 1 sierpnia 2018 r. w sprawie wprowadzenia Polityki ochrony danych osobowych Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, Instrukcji zarządzania siecią i systemami informatycznymi w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Regulaminu monitoringu wizyjnego w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Procedury fizycznego dostępu do pomieszczeń oraz dokumentów zawierających dane osobowe przechowywanych w wersji papierowej w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu oraz Procedury ochrony danych osobowych w badaniach naukowych prowadzonych w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu ze zmianami (zwanej dalej: Instrukcją) wprowadza się następujące zmiany:

1. w § 20, po ust. 11 dodaje się ust. 12 o następującym brzmieniu:

„12. W zakresie służbowej poczty elektronicznej udostępnionej poprzez stronę internetową Uczelni, obowiązuje uwierzytelnianie wieloskładnikowe (Multi-Factor Authentication), które wymaga zainstalowania odpowiedniej aplikacji. W aplikacji generują się czasowe hasła jednorazowe, umożliwiające zalogowanie do poczty elektronicznej, stanowiące drugą warstwę zabezpieczenia konta.”.

2. w § 23 ust. 1 po pkt 20) dodaje się punkt 20a) – 20f) o następującym brzmieniu:

„20a) W przypadku krótkotrwałej nieobecności użytkownika konta pocztowego, użytkownik stosuje autoodpowiedź/autoresponder zawierający informację o osobie zastępującej w czasie nieobecności, do której nadawca może przesłać wiadomość. Podaje przy tym: imię i nazwisko, numer telefonu do kontaktu i adres skrzynki pocztowej, na który możliwe jest przysyłanie korespondencji elektronicznej.

20b) W przypadku dłuższej nieobecności pracownika, w sytuacji braku zastosowania przez niego autoodpowiedzi/autorespondera, o którym mowa w pkt 20a, odpowiednia autoodpowiedź może zostać ustawiona przez CI na wniosek bezpośredniego przełożonego / kierownika jednostki użytkownika.

20c) W uzasadnionych przypadkach w trakcie nieobecności użytkownika, gdy jest to niezbędne do zachowania ciągłości zadań realizowanych przez Uczelnię, CI udostępnia bezpośredniemu przełożonemu / kierownikowi jednostki użytkownika treść korespondencji zgromadzonej na koncie pocztowym nieobecnego użytkownika, na zasadach określonych w pkt. 20 d i 20 e.

20d) Udostępnienie, o którym mowa powyżej następuje na pisemny wniosek bezpośredniego przełożonego / kierownika jednostki użytkownika, złożony do Zastępcy Dyrektora Generalnego ds. Organizacyjnych, po pozytywnym rozpatrzeniu wniosku. We wniosku należy wskazać w szczególności: adres e-mail, którego dotyczy udostępnienie, jednostkę organizacyjną, w której zatrudniony jest nieobecny użytkownik konta pocztowego, okres czasu, którego ma dotyczyć udostępniana korespondencja oraz uzasadnienie wniosku, w tym powód udostępnienia.

20e) Udostępnienie, w pierwszej kolejności następuje w formie zestawienia wiadomości zgromadzonych na koncie nieobecnego użytkownika, które obejmuje: tytuły, nadawców i odbiorców wiadomości. Na podstawie przedstawionego zestawienia, bezpośredni przełożony / kierownik jednostki użytkownika decyduje, które wiadomości są niezbędne do zachowania ciągłości zadań realizowanych w jednostce (zgodnie z uzasadnieniem opisanym we wniosku) i wskazuje je CI. CI udostępnia wyłącznie treść i załączniki do wiadomości wskazanych przez bezpośredniego przełożonego / kierownika jednostki użytkownika.

- 20f) Po powrocie użytkownika konta pocztowego do pracy, przywracany jest normalny obieg korespondencji i ustawienia skrzynki pocztowej.”.
3. w załączniku nr 12 do Instrukcji (Regulamin korzystania z systemu poczty elektronicznej Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu),wprowadza się następujące zmiany:
- 1) w pkt 2, po ppkt 2.16. dodaje się ppkt 2.16a. o następującym brzmieniu:
„2.16a. Drugą warstwę zabezpieczenia konta stanowi czasowe hasło jednorazowe, generowane przez odpowiednią aplikację (uwierzytelnianie wieloskładnikowe Multi-Factor Authentication). Rekomendowaną aplikacją służącą do uwierzytelniania dwuskładnikowego jest Microsoft Authenticator.”
 - 2) w pkt 2 ppkt 2.17 otrzymuje następujące brzmienie:
„2.17. W przypadku nieobecności należy ustawić autoodpowiedź/autoresponder, zawierający informację o osobie, która zastępuje użytkownika w czasie nieobecności, do której nadawca może przesłać wiadomość. Użytkownik podaje przy tym: imię i nazwisko, numer telefonu do kontaktu i adres skrzynki pocztowej, na który możliwe jest przysyłanie korespondencji elektronicznej.”.

§2

Zarządzenie wchodzi w życie z dniem podpisania.

Uniwersytet Medyczny we Wrocławiu
REKTOR
prof. dr hab. Piotr Ponikowski

Otrzymują:

według rozdzielnika

MM