

## **Zarządzenie Nr 70/2025**

Rektora Pomorskiego Uniwersytetu Medycznego w Szczecinie  
z dnia 16 kwietnia 2025 r. w sprawie wprowadzenia  
obowiązkowej weryfikacji wieloetapowej dla dostępu do  
wybranych systemów informatycznych Pomorskiego  
Uniwersytetu Medycznego w Szczecinie, wykorzystywanych do  
komunikacji studentów z Uczelnią drogą elektroniczną

Na podstawie art. 23 ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2024 r. poz. 1571 z późn. zm.) w związku z § 49 ust. 1 Statutu Pomorskiego Uniwersytetu Medycznego w Szczecinie, w trosce o zapewnienie odpowiedniego poziomu bezpieczeństwa systemów informatycznych oraz danych przetwarzanych i przechowywanych na Uczelni, zarządzam, co następuje:

### **§1**

#### **Obowiązek weryfikacji wieloetapowej**

1. Wprowadza się obowiązkową weryfikację wieloetapową (MFA – Multi Factor Authentication) dla dostępu do systemów informatycznych Uczelni, określonych w załączniku do niniejszego Zarządzenia, wykorzystywanych do komunikacji studentów z Uczelnią drogą elektroniczną.
2. W pierwszej kolejności zabezpieczenie MFA wprowadzone zostaje dla aplikacji środowiska Microsoft 365 w domenie [@student.pum.edu.pl](mailto:@student.pum.edu.pl), udostępnionej dla Pomorskiego Uniwersytetu Medycznego w Szczecinie. Zabezpieczenie wprowadzone zostaje dla wszystkich studentów Uczelni.

### **§2**

#### **Zakres obowiązywania**

1. Weryfikacja wieloetapowa (MFA) dotyczy wszystkich spersonalizowanych kont studentów w systemach informatycznych Uczelni, wykorzystywanych przez studentów do celów związanych z procesem dydaktycznym, obejmujących zarówno komunikację wewnętrzną, jak i korespondencję zewnętrzną oraz współdzielenie danych.

2. Wdrożenie mechanizmu uwierzytelniania wieloskładnikowego MFA ma na celu zwiększenie bezpieczeństwa informacji oraz ochronę przed nieautoryzowanym dostępem do systemów, przetwarzanych w nich danych oraz zgromadzonych na nich zasobów.

### **§3**

#### **Procedura konfiguracji MFA**

1. Każdy student Uczelni zobowiązany jest do skonfigurowania weryfikacji wieloetapowej na swoim personalnym koncie użytkownika w systemie informatycznym do dnia wskazanego w załączniku dla danego systemu.
2. Instrukcje dotyczące konfiguracji weryfikacji wieloetapowej MFA dla poszczególnych systemów oraz wsparcie techniczne będą dostępne na stronie <https://www.pum.edu.pl/mfa> oraz w Dziale Informatyki.

### **§4**

#### **Wykorzystanie urządzeń mobilnych do autoryzacji**

1. W celu zapewnienia bezpieczeństwa danych logowania, weryfikacja wieloetapowa wykorzystywać będzie urządzenia mobilne, w tym prywatne telefony komórkowe oraz smartfony studentów, jako narzędzie do potwierdzania tożsamości użytkownika.
2. Urządzenia, o których mowa w ust. 1, mają służyć wyłącznie jako dodatkowy, skuteczny mechanizm zabezpieczenia tożsamości cyfrowej użytkownika systemu informatycznego, chroniąc zasoby Uczelni przed nieautoryzowanym dostępem.
3. Student zachowuje pełną kontrolę nad swoim urządzeniem mobilnym, mając wyłączny dostęp do aplikacji Microsoft Authenticator, która jest zabezpieczona blokadą personalną, co zapewnia dodatkową warstwę ochronną jego cyfrowej tożsamości. Dodatkowo, wykorzystanie urządzenia mobilnego do autoryzacji ułatwia odzyskiwanie dostępu do konta, w przypadku utraty hasła dostępowego.

### **§5**

#### **Utrzymanie dostępu**

1. Brak konfiguracji weryfikacji wieloetapowej (MFA) w wyznaczonym terminie dla wskazanego w załączniku do niniejszego Zarządzenia systemu informatycznego

spowoduje tymczasowe zablokowanie dostępu do danego systemu informatycznego i udostępnionych w jego ramach usług.

2. Dostęp zostanie uzyskany po przeprowadzeniu przez użytkownika procesu konfiguracji i aktywacji mechanizmu dodatkowego uwierzytelniania.

## **§6**

### **Odpowiedzialność**

1. Weryfikacja wieloetapowa zwiększa bezpieczeństwo i chroni konta przed nieautoryzowanym dostępem nawet w przypadku, jeśli hasło zostanie przejęte.
2. Wszystkie informacje o włączonych mechanizmach ochronnych, prywatnym numerze telefonu oraz prywatnym adresie e-mail przechowywane są w profilu na koncie danego użytkownika, dostęp do nich wymaga dodatkowego logowania i zastrzeżony jest wyłącznie dla właściciela konta.
3. Każdy student jest odpowiedzialny za utrzymanie aktualnych danych kontaktowych w systemie (tzn. numeru telefonu oraz pomocniczego adresu e-mail).

## **§7**

### **Wprowadzanie MFA dla kolejnych systemów informatycznych**

1. Kolejne systemy informatyczne wykorzystywane na Uczelni objęte uwierzytelnianiem wieloskładnikowym będą uzupełniać listę stanowiącą załącznik do niniejszego zarządzenia.
2. Wprowadzenie dla kolejnych systemów zabezpieczeń MFA zostanie ogłoszone w formie komunikatu Rektora informującego o wprowadzeniu zabezpieczenia dla wskazanego systemu informatycznego oraz o uzupełnieniu załącznika do niniejszego zarządzenia.

## **§8**

### **Kampania informacyjna**

1. Każdy student będący użytkownikiem systemu objętego niniejszym zarządzeniem otrzyma drogą mailową powiadomienie o obowiązku wdrożenia weryfikacji wieloetapowej (MFA) oraz terminie jej konfiguracji.
2. Wprowadzenie MFA jest zgodne z najlepszymi praktykami w zakresie cyberbezpieczeństwa zalecanymi przez Europejską Agencję ds.

Cyberbezpieczeństwa (ENISA), NIST (National Institute of Standards and Technology) oraz Microsoft Security Standards.

3. Wdrożenie weryfikacji wieloetapowej (MFA) ma na celu zabezpieczenie Uczelni przed nadużyciami, ochronę przetwarzanych i przechowywanych przez Uczelnię danych przed zewnętrznymi zagrożeniami cyfrowymi, a także podwyższenie poziomu bezpieczeństwa oraz spełnienie wymogów prawnych i organizacyjnych dotyczących ochrony informacji.

**§9**

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od dnia 9 kwietnia 2025 r.

**prof. dr hab. Leszek Domański**  
**Rektor PUM**

Lista systemów informatycznych Pomorskiego Uniwersytetu Medycznego w Szczecinie udostępniających uwierzytelnianie wieloskładnikowe MultiFactor Authentication (MFA) oraz terminy wprowadzenia mechanizmu MFA.

| Ip | Nazwa systemu       | Adres URL                                                                           | Data wprowadzenia MFA <sup>1)</sup> |
|----|---------------------|-------------------------------------------------------------------------------------|-------------------------------------|
| 1  | Microsoft 365       | <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> | 22 kwietnia 2025 r.                 |
| 2  | Wirtualny Dziekanat | <a href="https://wd.pum.edu.pl">https://wd.pum.edu.pl</a>                           | 9 kwietnia 2025 r.                  |
| 3  | ...                 |                                                                                     |                                     |

- 1) Data wprowadzenia MFA określa graniczny termin, do którego każdy użytkownik danego systemu jest zobowiązany aktywować uwierzytelnianie wieloskładnikowe MFA zgodnie z instrukcją.

W sytuacji, gdy użytkownik nie wykona powyższego polecenia, konto dostępowe będzie tymczasowo blokowane do czasu zrealizowania wymogu.

