DOP.020.56.2025

Zarządzenie Nr 56/2025

Rektora Pomorskiego Uniwersytetu Medycznego w Szczecinie z dnia 27 marca 2025 r. w sprawie wprowadzenia obowiązkowej weryfikacji wieloetapowej dla dostępu do służbowej poczty elektronicznej w systemie Microsoft 365 oraz systemów informatycznych na Pomorskim Uniwersytecie Medycznym w Szczecinie

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 cyberbezpieczeństwa systemów informacyjnych i danych przechowywanych i przetwarzanych 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 realizacji zadań służbowych.
2. W pierwszej kolejności i w szczególności zabezpieczenie MFA wprowadzone zostaje dla służbowej poczty elektronicznej, obsługiwanej na Pomorskim Uniwersytecie Medycznym w Szczecinie za pomocą systemu Microsoft 365. Zabezpieczenie wprowadzone zostaje dla wszystkich pracowników i współpracowników Uczelni.

§2

Zakres obowiązywania

1. Weryfikacja wieloetapowa (MFA) dotyczy wszystkich spersonalizowanych kont użytkowników w systemach informatycznych wykorzystywanych przez pracowników do celów służbowych, obejmujących zarówno komunikację wewnętrzną, jak i korespondencję z instytucjami zewnętrznymi oraz współdzielenie danych i przesyłanie danych służbowych i poufnych.
2. Wdrożenie mechanizmu uwierzytelniania wieloskładnikowego MFA ma na celu zwiększenie bezpieczeństwa informacji oraz ochronę przed nieautoryzowanym dostępem do systemów, zasobów i danych organizacji.

§3
Procedura konfiguracji MFA

1. Każdy pracownik 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 będzie mogła wykorzystywać urządzenia mobilne, w tym prywatne telefony komórkowe i smartfony pracowników, wyłącznie jako narzędzie do autoryzacji.
2. Pracodawca **nie wymaga** od pracownika korzystania z prywatnych urządzeń mobilnych – decyzja o ich użyciu należy wyłącznie do użytkownika. Urządzenia te mają służyć wyłącznie jako dodatkowy i skuteczny mechanizm zabezpieczenia tożsamości cyfrowej użytkownika, chroniąc przed nieautoryzowanym dostępem i próbami przejęcia konta służbowego.
3. Pracownik zachowuje pełną kontrolę nad swoim urządzeniem mobilnym, mając wyłączny dostęp do kodów weryfikacyjnych, co zapewnia dodatkową warstwę ochrony jego służbowej tożsamości cyfrowej. Dodatkowo, wykorzystanie urządzenia mobilnego do autoryzacji może znacząco ułatwić odzyskiwanie dostępu do konta w przypadku zapomnienia hasła lub jego zmiany.
4. W przypadku braku dostępu do urządzenia mobilnego lub niemożności skorzystania z tej metody, pracownik ma obowiązek niezwłocznego zgłoszenia tego faktu do Działu Informatyki w celu ustalenia alternatywnego rozwiązania uwierzytelniającego.

§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 co za tym idzie do jego usług.
2. Dostęp zostanie uzyskany po przeprowadzeniu przez użytkownika procesu konfiguracji i aktywacji mechanizmu dodatkowego uwierzytelniania.

§6
Odpowiedzialność

1. Weryfikacja wieloetapowa znacząco zwiększa bezpieczeństwo i chroni konta przed nieautoryzowanym dostępem, nawet jeśli hasło zostanie przejęte.
2. Każdy pracownik jest odpowiedzialny za utrzymanie aktualnych danych kontaktowych w systemie (tzn. numeru telefonu, pomocniczego adresu e-mail)
3. Każdy pracownik zobligowany jest do przestrzegania zasad bezpieczeństwa; w szczególności zasad dotyczących korzystania z poczty elektronicznej, określonych zarządzeniem Rektora Nr 32/2024 z dnia 24 kwietnia 2024 roku.

§7
Kary i sankcje

Niedostosowanie się do Zarządzenia lub nieprzestrzeganie zasad bezpieczeństwa dostępu do systemów informatycznych Uczelni może skutkować podjęciem działań dyscyplinarnych zgodnie z obowiązującymi przepisami wewnętrznymi Uczelni.

§8
Wprowadzanie MFA dla kolejnych systemów Informatycznych

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

§9
Kampania informacyjna

1. Każdy użytkownik systemu objętego niniejszym zarządzeniem otrzyma powiadomienie drogą mailową 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. Obowiązek konfiguracji weryfikacji wieloetapowej (MFA) to kluczowy krok w kierunku podniesienia poziomu bezpieczeństwa organizacji i ochrony przed zagrożeniami cyfrowymi.

4. Wdrożenie tego mechanizmu ma na celu zapewnienie integralności, poufności i dostępności danych, a także spełnienie wymogów prawnych i organizacyjnych dotyczących ochrony informacji.

§10

Zarządzenie wchodzi w życie z dniem podpisania.

prof. dr hab. Leszek Domański

Rektor PUM

DOP.020.56.2025

Załącznik do Zarządzenia Rektora Nr 56/2025

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

lp	Nazwa systemu	Adres URL	Data wprowadzenia MFA [1)]
1	Microsoft 365	https://login.microsoftonline.com/	27 marca 2025 r.
2	Portal WWW PUM	https://www.pum.edu.pl	31 marca 2025 r.
3			
4			
5			
6			
7			

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.