ZARZĄDZENIE Nr 4/2025
Rektora Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie
z dnia 16 stycznia 2025 r.

w sprawie wprowadzenia dodatkowych zabezpieczeń
przed nieautoryzowanym dostępem do systemów informatycznych UKSW

Na podstawie § 25 ust. 2 pkt 1 lit. b Statutu Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, w związku z art. 24 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), zarządza się, co następuje:

§ 1.

1. Wprowadza się wyższy poziom kontroli dostępu i uwierzytelniania w celu zarządzania ryzykiem dla bezpieczeństwa i ochrony przed nieautoryzowanym dostępem do systemów informatycznych Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, zwanego dalej „UKSW" lub „Uniwersytetem", wykorzystywanych do przetwarzania danych osobowych oraz innych ważnych zasobów informacyjnych w prowadzonej działalności Uniwersytetu.
2. Zapewnienie dostępu wyłącznie uprawnionym Użytkownikom ma na celu zapobieganie wpływowi incydentów na odbiorców usług lub inne świadczone usługi, bądź minimalizowanie takiego wpływu co stanowi jeden z najważniejszych obowiązków Administratora Danych.

§ 2.

Zobowiązuje się wszystkie osoby korzystające z systemów informatycznych UKSW, zwanych dalej „Użytkownikami" do zastosowania mechanizmu silnego uwierzytelniania w postaci weryfikacji dwuetapowej, jako ochronę przed phishingiem, socjotechniką i kradzieżą uwierzytelnień.

§ 3.

1. Weryfikacja dwuetapowa (2FA) to proces, w którym Użytkownik oprócz swojego loginu i hasła musi podać także dodatkowy kod. Kod jest generowany i dostarczony dla Użytkownika niezależną aplikacją np. Microsoft Authenticator lub Google Authenticator.
2. W celu uzyskania dostępu do usług i danych UKSW, Użytkownik musi przejść przez dwa etapy:
   1) przy pierwszym logowaniu pod adresem strony: *logowanie.uksw.edu.pl*, Użytkownik zostanie poproszony o skonfigurowanie tzw. autentykatora, czyli aplikacji generującej kody jednorazowe. System logowania wyświetli szczegółową instrukcję, jak to zrobić. Konieczne będzie uprzednie

pobranie i zainstalowanie na swoim urządzeniu mobilnym jednej z aplikacji, o której mowa w ust. 1;

2) następnie należy otworzyć aplikację, stworzyć nowy autentykator poprzez zeskanowanie wyświetlonego na ekranie kodu QR i podać zwrotnie krótki kod wygenerowany przez autentykator.

3. Od momentu skonfigurowania autentykatora, przy kolejnych logowaniach stosowany będzie dodatkowy składnik uwierzytelniania – po podaniu identyfikatora i hasła, system zapyta o kod jednorazowy. Należy wtedy otworzyć aplikację autentykatora, odnaleźć krótki kod i przepisać go do aplikacji logowania.

4. System weryfikacji pozwala na zapamiętanie konkretnego urządzenia (np. przeglądarki internetowej) jako zaufanego – na takim urządzeniu pytanie o kod nie będzie pojawiać się za każdym razem.

5. W sytuacji utraty autentykatora, nie będzie możliwości zalogowania się do usług UKSW. Należy brać to pod uwagę w przypadku np. planowanej wymiany telefonu.

6. System umożliwia posiadanie więcej niż jednego autentykatora, przed zmianą urządzenia – należy skonfigurować dodatkowy identyfikator na nowym urządzeniu.

7. W sytuacji utraty dostępu do autentykatora (np. w przypadku kradzieży lub awarii telefonu), jedyną metodą odzyskania dostępu do konta i usług UKSW będzie osobisty kontakt z Centrum Systemów Informatycznych UKSW w celu niezbędnej weryfikacji Użytkownika na postawie dokumentu tożsamości.

8. Użytkownicy mają obowiązek zgłaszać wszelkie sytuacje, które:
   1) wskazują potencjalne ryzyko lub naruszenie bezpieczeństwa zasobów informatycznych, bezpośrednio do CSI poprzez formularz zgłoszeniowy (https://csi.uksw.edu.pl/zgloszenie);
   2) stanowią incydenty i naruszenia bezpieczeństwa danych osobowych zgodnie z Procedurą postępowania z naruszeniami w UKSW, bezpośrednio do Inspektora Ochrony Danych UKSW, za pomocą formularza dostępnego na stronie głównej UKSW, w zakładce Ochrona Danych Osobowych, w menu zgłaszanie naruszeń.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

ks. prof. dr hab. Ryszard Czekalski