BR.0210.1.58.2023

Zarządzenie nr 58
Rektora Uniwersytetu w Białymstoku
z dnia 26 września 2023 r.

w sprawie zdalnego dostępu do systemów teleinformatycznych Uniwersytetu w Białymstoku

Na podstawie § 17 ust. 4 pkt 2 Statutu Uniwersytetu w Białymstoku zarządzam, co następuje:

§ 1

Zarządzenie ustala zasady zdalnego dostępu do zasobów teleinformatycznych Uniwersytetu w Białymstoku, zwanych dalej „zasobami teleinformatycznymi".

§ 2

1. Zdalny dostęp do zasobów teleinformatycznych jest realizowany za pomocą usług VPN i certyfikatów znajdujących się na kluczach sprzętowych.
2. Kanclerz powołuje i odwołuje:
   1) Administratora Kluczy,
   2) Administratora Serwera Certyfikacji,
   3) Administratora Serwera VPN.

§ 3

1. Decyzję o nadaniu/odebraniu pracownikowi Uniwersytetu zdalnego dostępu do zasobów teleinformatycznych podejmuje kanclerz na wniosek kierownika jednostki organizacyjnej. Wzór wniosku stanowi Załącznik do niniejszego Zarządzenia.
2. Korzystanie przez pracownika ze zdalnego dostępu do zasobów teleinformatycznych poza siedzibą uczelni odbywa się za zgodą pracodawcy.

§ 4

Po podjęciu decyzji o nadaniu pracownikowi uprawnienia do zdalnego dostępu do zasobów teleinformatycznych:

1) Administrator Kluczy przygotowuje klucz sprzętowy,
2) Administrator Serwera Certyfikacji zatwierdza wydanie certyfikatu,
3) Administrator Serwera VPN przypisuje certyfikat w systemie VPN.

§ 5

1. Upoważniony pracownik odbiera osobiście klucz sprzętowy u Administratora Kluczy potwierdzając odbiór własnoręcznym podpisem.
2. Klucz sprzętowy może być używany wyłącznie przez upoważnionego pracownika.
3. Uwierzytelnianie do zasobów teleinformatycznych realizowane jest za pomocą certyfikatu znajdującego się na kluczu sprzętowym oraz unikatowego hasła znanego jedynie upoważnionemu pracownikowi.
4. Klucz sprzętowy oraz unikatowe hasło nie mogą być udostępniane osobom trzecim.
5. W razie zgubienia lub kradzieży klucza sprzętowego, pracownik zobowiązany jest do natychmiastowego zgłoszenia incydentu bezpieczeństwa do Administratora Serwera Certyfikacji.

§ 6

1. Zdalny dostęp do zasobów teleinformatycznych może zostać nadany, za zgodą kanclerza, pracownikom podmiotu zewnętrznego.
2. Zdalny dostęp, o którym mowa w ust. 1, nadaje się w celu przeprowadzenia prac serwisowych, uruchomienia zdalnej sesji terminalowej lub innego oprogramowania penetracyjnego z serwisowanego serwera.
3. Prace, o których mowa w ust. 2, mogą być realizowane wyłącznie pod nadzorem ASI.

§ 7

Administrator Kluczy prowadzi rejestr zdalnego dostępu do systemów teleinformatycznych Uniwersytetu w Białymstoku.

§ 8

Za czynności techniczne związane z nadaniem dostępu do zasobów teleinformatycznych, znajdujących się w Uniwersytecie w Białymstoku oraz systemów

informatycznych, funkcjonujących w Uniwersytecie w Białymstoku odpowiedzialny jest Administrator Systemów Informatycznych (ASI).

§ 9

Osoba korzystająca ze zdalnego dostępu do zasobów teleinformatycznych jest zobowiązana do przestrzegania Instrukcji zarządzania systemem informatycznym w Uniwersytecie w Białymstoku, określonej w odrębnych przepisach.

§ 10

1. Korzystanie przez pracownika ze zdalnego dostępu do zasobów teleinformatycznych jest realizowane z wykorzystaniem sprzętu komputerowego będącego własnością uczelni.
2. Sprzęt komputerowy, na którym realizowany jest zdalny dostęp do zasobów teleinformatycznych, powinien być objęty ochroną antywirusową i zabezpieczeniem dostępu sieciowego.
3. Sprzęt komputerowy, na którym realizowany jest zdalny dostęp do zasobów teleinformatycznych, nie może być udostępniany osobom trzecim.

§ 11

1. Zdalny dostęp do zasobów teleinformatycznych powinien być realizowany poprzez wykorzystanie zaufanych internetowych punktów dostępowych, w bezpiecznym otoczeniu, minimalizującym zagrożenia m.in. napadu, kradzieży oraz możliwości podejrzenia przetwarzanych informacji przez osoby nieuprawnione.
2. Po zakończeniu korzystania ze zdalnego dostępu do zasobów teleinformatycznych należy zamknąć połączenie VPN.

§ 12

Naruszenie bezpieczeństwa zdalnego dostępu do systemów teleinformatycznych jest traktowane jako naruszenie obowiązków służbowych i może skutkować odpowiedzialnością dyscyplinarną.

§ 13

Odebranie uprawnienia do zdalnego dostępu do systemów teleinformatycznych, tj. zablokowanie konta VPN lub unieważnienie certyfikatu następuje:

1) gdy zakończy się okres, na który uprawnienie zostało przyznane,
2) decyzją kanclerza,

3) z dniem rozwiązania umowy o pracę,
4) na skutek kompromitacji certyfikatu, tj. upublicznienia klucza prywatnego znajdującego się na kluczu sprzętowym,
5) na wniosek kierownika jednostki organizacyjnej.

§ 14

1. Klucz sprzętowy jest własnością Uniwersytetu w Białymstoku.
2. Klucze sprzętowe pracowników administracji centralnej są finansowane ze środków ogólnouczelnianych.
3. Klucze sprzętowe pracowników jednostek organizacyjnych są finansowane ze środków własnych jednostek, z zastrzeżeniem ust. 4.
4. Klucze sprzętowe dziekanów wydziałów, dyrektorów instytutów i dyrektora filii są finansowane ze środków ogólnouczelnianych.

§ 15

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor
Uniwersytetu w Białymstoku
Prof. dr hab. Robert W. Ciborowski

Załącznik
do Zarządzenia nr 58
Rektora Uniwersytetu w Białymstoku
z dnia 26 września 2023 r.

…… ……

jednostka organizacyjna *Miejscowość, data*

Kanclerz

Uniwersytetu w Białymstoku

Wniosek o nadanie/odebranie

zdalnego dostępu do systemów informatycznych Uniwersytetu w Białymstoku

Dane pracownika

Imię i nazwisko	
Jednostka organizacyjna	
Służbowy adres e-mail	
Telefon kontaktowy	
Zakres dostępu*	[USOS, EZD, XEMI, DAK, DSK, inne (*opisać jaki*)]
Termin dostępu	od ……. do ……

* *zaznaczyć właściwe*

Opłata za wydanie certyfikatu zostanie pokryta ze środków własnych jednostki/środków ogólnouczelnianych/ innych (jakich?) * …….

……

podpis kierownika jednostki organizacyjnej

Decyzja kanclerza

……

……

podpis

Potwierdzenie odbioru klucza sprzętowego

Klucz sprzętowy odebrałam/odebrałem dnia ……..,

…..……..……...

podpis upoważnionego pracownika