

**Zarządzenie nr 41/2022
z dnia 01 czerwca 2022 r.**

**w sprawie realizacji zadań wynikających z wprowadzenia drugiego stopnia alarmowego
(2. stopień BRAVO) i trzeciego stopnia alarmowego CRP (3. stopień CHARLIE-CRP)
na całym terytorium Rzeczypospolitej Polskiej**

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. 2022 poz. 574, z późn. zm.) w związku z zarządzeniem nr 153 Prezesa Rady Ministrów z dnia 31 maja 2022 roku w sprawie wprowadzenia drugiego stopnia alarmowego (2. stopień BRAVO) na całym terytorium Rzeczypospolitej Polskiej oraz zarządzenia nr 154 Prezesa Rady Ministrów z dnia 31 maja 2022 roku w sprawie wprowadzenia trzeciego stopnia alarmowego CRP (3. stopień CHARLIE-CRP) na całym terytorium Rzeczypospolitej Polskiej zarządzam, co następuje:

§ 1

1. Kierownicy jednostek organizacyjnych Państwowej Uczelni Angelusa Silesiusa zobowiązani są zapewnić funkcjonowanie podległych im jednostek, ze szczególnym uwzględnieniem realizacji zadań wynikających z wprowadzenia drugiego stopnia alarmowego (2. stopień BRAVO) na całym terytorium Rzeczypospolitej Polskiej oraz trzeciego stopnia alarmowego CRP (3. stopień CHARLIE-CRP) na całym terytorium Rzeczypospolitej Polskiej, tj.:
 - 1) wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych uczelni oraz:
 - a) monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
 - b) sprawdzać dostępność usług elektronicznych,
 - c) dokonywać, w razie potrzeby, zmian w dostępie do systemów;
 - 2) poinformować pracowników i studentów o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności osoby odpowiedzialne za bezpieczeństwo systemów;
 - 3) dokonać przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP, w szczególności dokonać weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych kluczowych dla funkcjonowania uczelni oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu;
 - 4) sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
 - 5) zapewnić dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych;
 - 6) przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku.

§ 2

Kierownik jednostki organizacyjnej niezwłocznie informuje Rektora o wystąpieniu okoliczności uniemożliwiających prawidłowe funkcjonowanie jednostki organizacyjnej, stanowiących zagrożenie bezpieczeństwa pracowników i studentów lub mienia w znacznych rozmiarach oraz incydentów mających wpływ na bezpieczeństwo systemów teleinformatycznych.

§ 3

Zarządzenie obowiązuje od dnia 01 czerwca 2022 roku, od godz. 00:00, do dnia 30 czerwca 2022 roku do godz. 23:59.

Rektor
prof. dr hab. Robert Wiszniowski