

ZARZĄDZENIE Nr 2/2024
Rektora Akademii Górniczo-Hutniczej
im. Stanisława Staszica w Krakowie
z dnia 2 stycznia 2024 r.

w sprawie zmiany Zarządzenia nr 16/2023 Rektora Akademii
Górnictwo-Hutniczej im. Stanisława Staszica w Krakowie z dnia 31 marca 2023 r.
w sprawie utworzenia Sektora IT i określenia zasad jego działania

Działając na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2023 r. poz. 742 z późn. zm.) oraz na podstawie §21 ust. 3 Statutu AGH (uchwała nr 123/2023 Senatu AGH z dnia 27 września 2023 r.), zarządzam co następuje:

§ 1.

1. W Zarządzeniu nr 16/2023 Rektora Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie z dnia 31 marca 2023 r. w sprawie utworzenia Sektora IT i określenia zasad jego działania, wprowadza się następujące zmiany:

1) w §2:

a) dodaje się ust. 1a w następującym brzmieniu:

„1a. Organizacja i realizacja działań dotyczących zwiększania poziomu bezpieczeństwa informacji oraz cyberbezpieczeństwa w Uczelni oraz koordynacja działań realizowanych przez jednostki organizacyjne.”;

b) dodaje się ust. 8a w następującym brzmieniu:

„8a. Analizowanie potrzeb Uczelni związanych z podnoszeniem poziomu bezpieczeństwa informacji oraz cyberbezpieczeństwa, w tym w zakresie wymagań prawnych i kontraktowych.”

c) ust. 9 otrzymuje brzmienie:

„9. Działalność doradcza i usługowa dla Władz Uczelni, jednostek AGH oraz podmiotów zewnętrznych w zakresie zarządzania, informatyzacji, projektowania, wdrażania i utrzymywania rozwiązań informatycznych oraz bezpieczeństwa informacji.

2) w §3 ust. 1 dodaje się lit. d w następującym brzmieniu:

„d) Centrum Bezpieczeństwa Informacji.”;

3) §4 ust. 2 lit. d otrzymuje brzmienie:

„d) rozdział zadań i kompetencji pomiędzy jednostki Sektora IT, w tym powoływanie oraz odwoływanie zespołów zadaniowych;”

4) §4 ust. 2 lit. h otrzymuje brzmienie:

„h) przedstawianie wyników analiz i sugestii Władzom Uczelni i jednostek organizacyjnych do wykorzystania przy opracowaniu rozwoju informatyzacji oraz zasad bezpieczeństwa teleinformatycznego Uczelni;”

5) uchyla się §5 ust. 5;

6) §6 ust. 1 lit. a otrzymuje brzmienie:

„a) zarządzanie infrastrukturą oraz wspieranie bezpieczeństwa teleinformatycznego w ramach współpracy z jednostkami AGH i podmiotami zewnętrznymi,”

7) uchyla się §6 ust. 2 lit. g;

8) §8 ust. 3 otrzymuje brzmienie:

„3. Rektor może powołać zastępców Dyrektora CZW, na wniosek Dyrektora ds. IT.”

9) §11 ust. 3 otrzymuje brzmienie:

„3. Rektor może powołać zastępców Dyrektora CWI, na wniosek Dyrektora ds. IT.”

10)po §13 dodaje się §13a, 13b, 13c w następującym brzmieniu:

„§13a

CENTRUM BEZPIECZEŃSTWA INFORMACJI

1. Centrum Bezpieczeństwa Informacji (CBI) jest jednostką pomocniczą, należącą do grupy centrów administracyjnych w administracji centralnej w rozumieniu regulaminu Organizacyjnego AGH, wchodzącą w skład Sektora IT.

2. Działalnością CBI kieruje Dyrektor CBI, podlegający bezpośrednio Dyrektorowi ds. IT. Dyrektora CBI powołuje i odwołuje Rektor, na wniosek Dyrektora ds. IT.
3. Rektor może powołać zastępców Dyrektora CBI, na wniosek Dyrektora ds. IT.
4. Wewnętrzną strukturę CBI określa Dyrektor ds. IT w zależności od okoliczności i potrzeb. Struktura CBI podlega zatwierdzeniu przez Rektora w zakresie powoływania wewnętrznych jednostek zgodnie z Regulaminem Organizacyjnym.

§ 13b

ZADANIA CBI

1. CBI wykonuje działalność operacyjną w zakresie zapewniania bezpieczeństwa, w tym bezpieczeństwa informatyzacji (cyfryzacji) oraz cyberbezpieczeństwa AGH.
2. Do zasadniczych zadań CBI należy:
 - a) zarządzanie bezpieczeństwem teleinformatycznym Uczelni;
 - b) działalność doradcza i wspierająca w zakresie projektowania, wdrażania rozwiązań z zakresu bezpieczeństwa informacji oraz podnoszenia poziomu cyberbezpieczeństwa Uczelni;
 - c) rozwój i dostarczanie usług z zakresu bezpieczeństwa.
3. Zadania CBI w szczególności obejmują:
 - a) współdziałanie z pozostałymi jednostkami Sektora IT w zakresie zapewniania bezpieczeństwa teleinformatycznego systemów Uczelni;
 - b) monitorowanie aktywności i podatności w sieciach i systemach informatycznych Uczelni;
 - c) testy zabezpieczeń systemów wykorzystywanych przez AGH;
 - d) obsługę incydentów bezpieczeństwa;
 - e) pomoc przy doborze i wdrażaniu systemów zabezpieczeń;
 - f) planowanie rozwoju i eksploatacji systemów cyberbezpieczeństwa wdrażanych i utrzymywanych w AGH;
 - g) określanie wytycznych, tworzenie polityk, zasad i procedur dotyczących cyberbezpieczeństwa w jednostkach organizacyjnych, w tym koordynowanie wdrażania ich w Uczelni oraz współtworzenie procedur dotyczących przestrzegania bezpieczeństwa informacji;
 - h) wyznaczanie zadań z obszaru podnoszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa Uczelni, do wykonania przez jednostki;
 - i) opiniowanie zasad dostępu i korzystania z Uczelnianej Sieci Komputerowej w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa;
 - j) analizowanie potrzeb Uczelni związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem, w tym w zakresie wymagań prawnych i kontraktowych;
 - k) opiniowanie (w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa) dostaw i usług sprzętu oraz oprogramowania dla jednostek AGH w szczególności systemów o zasięgu ogólnouczelnianym;
 - l) prowadzenie działań w zakresie analizy złośliwego oprogramowania, obsługi incydentów, informatyki śledczej dla podmiotów zewnętrznych;
 - m) realizowanie oferty doradczej, szkoleniowej i edukacyjnej w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa dla jednostek Uczelni, pracowników Uczelni oraz podmiotów zewnętrznych;
 - n) przygotowywanie planów, analiz, opinii i ekspertyz z zakresu cyberbezpieczeństwa.

§ 13c

DYREKTOR CBI

1. Dyrektor odpowiada za funkcjonowanie CBI, we wszystkich aspektach jego działalności. Do głównych zadań Dyrektora CBI należy:
 - a) zarządzanie CBI jako jednostką organizacyjną AGH, na zasadach określonych prawem w tym prawem wewnętrznym AGH, z uwzględnieniem niniejszego zarządzenia oraz upoważnienia udzielonego przez Rektora;
 - b) planowanie, koordynowanie i nadzorowanie pracy działów CBI realizujących zadania;
 - c) organizacja bieżącej działalności CBI oraz zarządzanie pracownikami i zasobami materialnymi przypisanymi do CBI;
 - d) przedstawianie Dyrektorowi ds. IT rocznych sprawozdań z działalności CBI.

2. Dyrektor CBI w szczególności:
- a) jest bezpośrednim przełożonym wszystkich pracowników zatrudnionych w CBI,
 - b) składa do Dyrektora ds. IT wnioski w sprawach zatrudnienia i zmian warunków umów podległych pracowników,
 - c) jest dysponentem środków finansowych przewidzianych w planie rzeczowo-finansowym AGH na realizację zadań CBI, w zakresie określonym pełnomocnictwem Rektora,
 - d) odpowiada za przygotowanie projektu planu rzeczowo-finansowego CBI i jego wykonanie,
 - e) sprawuje nadzór nad racjonalną gospodarką mieniem Uczelni zgromadzonym w CBI,
 - f) planuje i nadzoruje racjonalne wykorzystanie zasobów lokalowych CBI,
 - g) sprawuje nadzór nad terminową realizacją ustaleń, decyzji i obowiązującej sprawozdawczości.
3. Ze względu na zewnętrzne uwarunkowania rynkowe związane z funkcjonowaniem służb cyberbezpieczeństwa, Dyrektor CBI może zamiennie lub równolegle używać tytułu Chief Information Security Officer – CISO AGH.”

§ 2.

1. Ustala się tekst jednolity Zarządzenia nr 16/2023 Rektora Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie z dnia 31 marca 2023 r. w sprawie utworzenia Sektora IT i określenia zasad jego działania, z uwzględnieniem zmian wprowadzonych niniejszym zarządzeniem.
2. Tekst jednolity, o którym mowa w ust. 1, stanowi załącznik do niniejszego zarządzenia.

§ 3.

Niniejsze zarządzenie wchodzi w życie z dniem podpisania.

R E K T O R

prof. dr hab. inż. Jerzy Lis