

ZARZĄDZENIE NR 15/2025
Rektora-Komendanta Akademii Pożarniczej

z dnia 11 kwietnia 2025 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Akademii Pożarniczej

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, z późn. zm.) oraz § 14 ust. 3 Statutu Akademii Pożarniczej, zatwierdzonego decyzją nr 36 Ministra Spraw Wewnętrznych i Administracji z dnia 29 września 2023 r. (Dz. Urz. Min. Spraw Wew. i Ad. poz. 37) zarządza się, co następuje:

§ 1.

Wprowadza się Politykę Bezpieczeństwa Informacji w Akademii Pożarniczej, stanowiącą załącznik do zarządzenia.

§ 2.

Zobowiązuje się kierowników jednostek organizacyjnych Akademii Pożarniczej (dalej „APOż”) do zapoznania funkcjonariuszy i pracowników z Polityką Bezpieczeństwa Informacji w APOż.

§ 3.

Traci moc zarządzenie nr 25/18 Rektora-Komendanta SGSP z dnia 22 maja 2018 r. w sprawie ustalenia Polityki Bezpieczeństwa Informacji.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik

do zarządzenia nr 15/2025
Rektora-Komendanta APOż
z dnia 11 kwietnia 2025 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI**§ 1.****Cel wprowadzenia Polityki Bezpieczeństwa Informacji**

Polityka Bezpieczeństwa Informacji stanowi zapewnienie, że Rektor-Komendant APOż wspiera i kieruje bezpieczeństwem informacji zgodnie z wymaganiami właściwych przepisów prawa powszechnie obowiązującego oraz regulacji wewnętrznych.

§ 2.**Znaczenie bezpieczeństwa informacji dla APOż**

1. Informacja oraz wspierające ją procesy i systemy są ważnymi aktywami APOż.
2. APOż i jej systemy informacyjne są narażone na zagrożenia bezpieczeństwa z wielu różnych źródeł, łącznie z przestępstwami z użyciem komputera, szpiegostwem, sabotażem, wandalizmem, pożarem czy powodzią.
3. Ochrona informacji przed szerokim spektrum zagrożeń ma zapewnić ciągłość działania APOż.

§ 3.**Zakres stosowania dokumentu Polityki Bezpieczeństwa Informacji**

1. Polityka Bezpieczeństwa Informacji ma zastosowanie w stosunku do wszystkich postaci informacji: dokumentów papierowych, zapisów elektronicznych i innych, będących własnością APOż lub
2. administrowanych przez APOż i przetwarzanych w systemach informatycznych, komunikacyjnych i aktach papierowych APOż.
3. Polityka Bezpieczeństwa Informacji, w zakresie bezpieczeństwa informacji w APOż, jest aktem nadrzędnym w stosunku do wszystkich innych obowiązujących w APOż regulacji.
4. Polityka Bezpieczeństwa Informacji ma zastosowanie w stosunku do wszystkich pracowników APOż (za pracownika APOż, w rozumieniu niniejszego dokumentu, uważa się także strażaka pełniącego
5. służbę w APOż), innych osób zatrudnionych w APOż, jak również osób trzecich mających dostęp do informacji w APOż.
6. Ochrona informacji wynikająca z Polityki Bezpieczeństwa Informacji jest realizowana na każdym etapie przetwarzania informacji.

§ 4.

Realizacja Polityki Bezpieczeństwa Informacji

1. Bezpieczeństwo informacji będzie osiąganе poprzez wdrażanie odpowiednich zabezpieczeń, o których mowa w § 7 ust. 2.
2. Zabezpieczenia będą ustanawiane, wdrażane, monitorowane, przeglądane, a w razie potrzeby zmieniane tak, aby spełnić poszczególne cele związane z bezpieczeństwem oraz prowadzoną działalnością statutową APOż.
3. Działania będą powiązane z pozostałymi procesami zarządzania funkcjonującymi w APOż.

§ 5.

Oświadczenie Rektora-Komendanta

1. Ochrona i bezpieczeństwo aktywów informacyjnych jest ważnym obszarem zarządzania APOż.
2. Rektor-Komendant APOż przywiązuje dużą wagę do kwestii związanych z bezpieczeństwem informacji oraz do wdrażania odpowiednich programów i mechanizmów jej ochrony.
3. Dokumenty Polityki Bezpieczeństwa Informacji stanowią kluczowy element strategii bezpieczeństwa APOż.
4. Rektor-Komendant APOż dąży do zredukowania ryzyka związanego z bezpieczeństwem aktywów informacyjnych do akceptowanego poziomu zachowując równowagę pomiędzy ryzykiem utraty bezpieczeństwa aktywów informacyjnych, a środkami przeznaczanymi na ich zabezpieczenia.
5. Każdy pracownik APOż jest zobowiązany zapoznać się z dokumentami Polityki Bezpieczeństwa Informacji, w zakresie go dotyczącym i przestrzegać postanowień zawartych w tych dokumentach i innych aktach z niego wynikających.

§ 6.

Zgodność z prawem, regulacjami wewnętrznymi i innymi wymaganiami

1. Punktem wyjścia do wdrożenia bezpieczeństwa informacji są zabezpieczenia wynikające z podstawowych wymogów prawa oraz praktyka uznana za powszechną w bezpieczeństwie informacji.
2. Najważniejszymi zabezpieczeniami dla APOż z prawnego punktu widzenia są:
 - 1) ochrona i poufność danych osobowych wynikające z 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 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
 - 2) ochrona zapisów APOż wynikających z ustawy z dnia 29 września 1994 r. o rachunkowości, innych przepisów prawa i regulacji wewnętrznych;
 - 3) ochrona prawa do własności intelektualnej wynikająca z ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych;

- 4) ochrona informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
3. Zabezpieczeniami uznawanymi za powszechną praktykę w zakresie bezpieczeństwa informacji są:
 - 1) zbiór dokumentów Polityki Bezpieczeństwa Informacji, w szczególności: Polityka Ochrony Danych Osobowych, Polityka Rachunkowości, Polityka Bezpieczeństwa Informacji Publicznej, Plan ochrony informacji niejawnych, Instrukcje Bezpieczeństwa i inne dokumenty związane z realizacją bezpieczeństwa informacji;
 - 2) przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji;
 - 3) uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji;
 - 4) poprawne przetwarzanie w aplikacjach;
 - 5) zarządzanie podatnościami technicznymi;
 - 6) zarządzanie ciągłością działania;
 - 7) reagowanie na incydenty związane z bezpieczeństwem informacji oraz minimalizacja ich skutków.

§ 7.

Zarządzanie ryzykiem utraty bezpieczeństwa aktywów informacyjnych APOż

1. Celem określenia i wdrożenia wymagań bezpieczeństwa aktywów informacyjnych w APOż wprowadza się okresowy powtarzalny proces szacowania ryzyka utraty bezpieczeństwa uwzględniający wszelkie zmiany mające wpływ na jego wynik.
2. APOż przyjmuje zasadę akceptowalnej równowagi, tj. nakłady na zabezpieczenia będą odpowiadać potencjalnym stratom, wynikającym z naruszenia bezpieczeństwa informacji.
3. Wyniki szacowania ryzyka będą wskazywać i określać adekwatne działania zarządcze, priorytety dla zarządzania ryzykiem bezpieczeństwa informacji oraz wdrożenie wybranych mechanizmów zabezpieczających.

§ 8.

Informacje przetwarzane w APOż

1. Podział informacji przetwarzanej w APOż przedstawia załącznik do Polityki Bezpieczeństwa Informacji w APOż.
2. Informacje uznane za chronione podlegają ochronie przed nieautoryzowanym: dostępem, powielaniem, ujawnieniem, modyfikacją, wykorzystaniem, zniszczeniem, jak również utratą, kradzieżą oraz zatajeniem.
3. Informacje jawne podlegają ochronie przed modyfikacją, utratą i zniszczeniem.
4. Dla informacji uznanej, jako chroniona oraz systemów przetwarzania zostaną opracowane polityki i instrukcje bezpieczeństwa oraz wynikające z nich regulaminy i procedury.

§ 9.

Zastosowanie zasad bezpieczeństwa informacji

Zasady zarządzania bezpieczeństwem informacji określone w dokumentach Polityki Bezpieczeństwa Informacji mają zastosowanie w stosunku do:

- 1) wszystkich pracowników, innych osób świadczących pracę na rzecz APOż, konsultantów, stażystów i innych osób mających dostęp do informacji podlegającej ochronie;
- 2) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są i lub będą informacje podlegające ochronie;
- 3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie;
- 4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

§ 10.

Dostęp do informacji chronionych

1. Każdy, kto ma uzyskać dostęp do informacji chronionej APOż, wynikający z zasady wiedzy koniecznej jest zobowiązany do:
 - 1) zapoznania się z przepisami wewnętrznymi APOż dotyczącymi zasad ochrony informacji;
 - 2) uczestniczenia w szkoleniu dotyczącym zasad ochrony informacji w APOż i zasad korzystania z systemów informatycznych;
 - 3) podpisania oświadczenia dotyczącego ochrony informacji w APOż;
 - 4) uzyskania uprawnień do przetwarzania informacji chronionej APOż.
2. Zakres nadanych uprawnień uzależniony jest od zakresu zadań realizowanych na danym stanowisku lub wynika z realizacji umowy.

§ 11.

Wymagania dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa informacji

1. Wszyscy pracownicy APOż, inne osoby świadczące pracę w APOż oraz, gdzie to jest wskazane, wykonawcy i użytkownicy reprezentujący stronę trzecią, będą odpowiednio przeszkoleni oraz regularnie informowani o uaktualnieniach obowiązujących w APOż polityk i procedur które są związane z realizowanymi zadaniami.
2. Szkolenia będą przeprowadzane przed przyznaniem dostępu do informacji lub usług i rozpoczynać się będą od formalnego procesu zapoznania się z polityką oraz wymaganiami bezpieczeństwa APOż.
3. Uświadamianie, kształcenie i szkolenie będzie dostosowane do zakresu realizowanych zadań i umiejętności osoby oraz będzie zawierało informacje na temat znanych zagrożeń, procedur

postępowania przy przetwarzaniu informacji oraz w przypadku zaistnienia incydentu związanego z bezpieczeństwem informacji.

§ 12.

Zarządzanie ciągłością

1. Celem zapewnienia zdolności APOż do nieprzerwanej realizacji zadań na akceptowalnym wcześniej zdefiniowanym poziomie po wystąpieniu zdarzenia zakłócającego ciągłość działania w APOż, został opracowany i wdrożony Plan Ciągłości Działania.
2. Za organizację i utrzymanie procesu zapewnienia ciągłości działania odpowiedzialny jest Rektor-Komendant.
3. Zadania w tym zakresie realizują kierowników pionów w poszczególnych obszarach funkcjonowania uczelni zgodnie z zakresami odpowiedzialności zdefiniowanymi w statucie APOż oraz regulaminie organizacyjnym APOż.

§ 13.

Konsekwencje naruszenia Polityki Bezpieczeństwa Informacji

Osoby naruszające zasady Polityki Bezpieczeństwa Informacji zostaną pociągnięte do odpowiedzialności służbowej (porządkowej, dyscyplinarnej) i karnej.

Załącznik

do Polityki Bezpieczeństwa Informacji w APOż

Podział informacji przetwarzanych w APOż

Informacja jawna	Informacja chroniona
<p>1. Informacja jawna wymagana przepisami prawa. (<i>Ustawa o dostępie do informacji publicznej, Ustawa o rachunkowości</i>)</p> <p>2. Informacja jawna związana z działalnością APOż</p> <p>3. Informacja reklamowa i marketingowa</p>	<p>1. Dane osobowe (<i>Ogólne Rozporządzenie o Ochronie Danych, Ustawa o ochronie danych osobowych</i>)</p> <p>2. Informacja niejawna (<i>Ustawa o ochronie informacji niejawnej</i>)</p> <p>3. Zapisy APOż (<i>Ustawa o rachunkowości, inne przepisy prawa, przepisy wewnętrzne APOż</i>)</p> <p>4. Informacja stanowiąca własność intelektualną (<i>Ustawa o prawie autorskim i prawach pokrewnych</i>)</p> <p>5. Informacja stanowiąca tajemnicę zawodową, m. in.:</p> <ul style="list-style-type: none">lekarską (<i>Ustawa o zawodzie lekarza</i>)psychologiczną (<i>ustawa o zawodzie psychologa i samorządzie zawodowym psychologów</i>)adwokacką-. (<i>Ustawa Prawo o adwokaturze</i>)radcy prawnego (<i>ustawa o radcach prawnych</i>) <p>6. informacje podlegające ochronie ze względów bezpieczeństwa</p>