Załącznik do zarządzenia rektora nr 79/2023
z dnia 22 czerwca 2023 roku
w sprawie: wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Polityka bezpieczeństwa informacji

Akademia Bialska
im. Jana Pawła II

AKADEMIA BIALSKA
IM. JANA PAWŁA II

WERSJA	1.1
KLAUZULA	JAWNE
ODBIORCY	Wszyscy pracownicy, współpracownicy, podmioty zewnętrzne
AKCEPTACJE	

Spis treści

DEFINICJE

Uczelnia lub AB – Akademia Bialska im. Jana Pawła II.

Rektor – Rektor Akademii Bialskiej im. Jana Pawła II.

Polityka – Polityka bezpieczeństwa informacji, niniejszy dokument.

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji.

Ryzyko – połączenie prawdopodobieństwa zdarzenia i jego konsekwencji. Ryzyko bezpieczeństwa informacji odnosi się do zdarzeń, które mogą negatywnie wpłynąć na osiągnięcie celów bezpieczeństwa informacji oraz na działalność AB.

Incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań operacyjnych i zagrażają bezpieczeństwu informacji.

I. POLITYKA UCZELNI

1. Wprowadzam zasady ochrony informacji, aby osiągnąć niezbędny, adekwatny do zagrożeń poziom bezpieczeństwa informacji w AB, w szczególności danych osobowych pracowników i studentów. Zasady ujęte w tym dokumencie mają być stosowane niezależnie od postaci i sposobu przetwarzania informacji.
2. Głównymi celami bezpieczeństwa informacji są:
    1) ochrona informacji przed udostępnieniem lub ujawnieniem ich nieupoważnionym osobom, podmiotom lub procesom (poufność) oraz przed nieuprawnionymi zmianami i manipulacjami (integralność),
    2) zapewnienie dostępu uprawnionym osobom, podmiotom i procesom do wszelkich informacji i usług, kiedy jest to wymagane (dostępność), w szczególności zapewnienie, że uczelnia będzie w stanie kontynuować świadczenie usług nawet w przypadku wystąpienia sytuacji awaryjnych,
    3) przypisanie odpowiedzialności za ochronę sprzętu i kluczowych informacji odpowiednim osobom w całym cyklu ich życia,
    4) utrzymanie zgodności z prawem i regulacjami bezpieczeństwa informacji, w tym ochrony danych osobowych (ochrona prywatności).
3. Deklaruję zapewnienie niezbędnych zasobów oraz wsparcie inicjatyw mających na celu osiągnięcie celów bezpieczeństwa.

4. Cele bezpieczeństwa informacji uczelnia osiąga m.in. przez:

   1) zapewnienie integracji bezpieczeństwa informacji z działalnością statutową i operacyjną uczelni,

   2) określenie ról organizacyjnych i przypisanie odpowiedzialności za bezpieczeństwo informacji,

   3) promowanie i motywowanie do odpowiedzialnego postępowania w zakresie bezpieczeństwa informacji wśród pracowników i współpracowników,

   4) podejmowanie skutecznych i efektywnych działań w oparciu o analizę ryzyka, w szczególności stosowanie adekwatnych do poziomu ryzyka zabezpieczeń technicznych i organizacyjnych,

   5) monitorowanie zmian w prawie i regulacjach oraz adekwatne dostosowywanie standardów, procedur, procesów i zabezpieczeń,

   6) skuteczne i efektywne zarządzanie incydentami bezpieczeństwa informacji oraz wyciąganie wniosków z ich przebiegu.

5. Niniejsza Polityka wprowadza system zarządzania bezpieczeństwem informacji i jest dokumentem nadrzędnym względem wszystkich wewnętrznych standardów dotyczących bezpieczeństwa informacji. Schemat regulacji (standardów) składających się na system zarządzania bezpieczeństwem informacji uczelni przedstawia Załącznik nr 1 do Polityki.

II. JAK STOSOWAĆ POLITYKĘ

1. Polityka i zasady przez nią wprowadzone obowiązują:

   1) wszystkich pracowników i współpracowników AB niezależnie od formy zatrudniania oraz inne osoby uzyskujące dostęp do informacji należących do uczelni,

   2) podmioty zewnętrzne realizujące działania lub współpracujące z uczelnią na podstawie umów i porozumień.

2. Politykę i zasady należy stosować względem wszystkich zasobów informacyjnych uczelni, w szczególności w stosunku do:

   1) istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych,

   2) zbiorów danych oraz nośników, na których te zbiory są zapisywane i przetwarzane niezależnie od typu nośnika,

3) siedziby i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

3. Politykę i zasady należy stosować łącznie ze standardami i procedurami bezpieczeństwa składającymi się na system zarządzania bezpieczeństwem informacji.

4. Polityka jest dokumentem jawnym. Celem jest zaznajomienie i stosowanie zasad Polityki przez wszystkich pracowników, współpracowników oraz podmioty zewnętrzne współpracujące z uczelnią. Z jawności wyłączone są dokumenty zależne od tj. standardy, procedury oraz zapisy operacyjne bezpieczeństwa.

5. Polityka, standardy oraz inne dokumenty zależne tworzą wspólnie system zarządzania bezpieczeństwem informacji. Utrzymanie systemu zarządzania uczelnia opiera o wymagania ISO/IEC 27001.

III. ROLE I ODPOWIEDZIALNOŚCI

Bezpieczeństwo informacji uczelnia organizuje w oparciu o następujące role organizacyjne oraz wskazanie konkretnych odpowiedzialności:

Rola	**Odpowiedzialność w zakresie bezpieczeństwa informacji**
Rektor i/lub inne wyznaczone osoby pełniące funkcje kierownicze	● akceptują i są sponsorami inicjatyw w zakresie bezpieczeństwa informacji ● wyznaczają Właścicieli procesów ● uczestniczą w procesie zarządzania ryzykiem ● określają poziom akceptowalnego ryzyka ● zatwierdzają Politykę i standardy
Inspektor bezpieczeństwa informacji	● inicjuje i koordynuje wdrażanie zabezpieczeń technicznych i organizacyjnych oraz przeglądy ryzyka ● koordynuje lub podejmuje reakcję na zdarzenia związane z bezpieczeństwem i incydenty ● konsultuje projekty i zmiany operacyjne ● monitoruje zmiany regulacyjne ● monitoruje działania dostawców usług ● koordynuje zarządzanie ciągłością działania uczelni
Inspektor Ochrony Danych Osobowych	● informuje rektora, podmioty przetwarzające oraz pracowników o obowiązkach spoczywających na nich wynikających z RODO ● monitoruje przestrzeganie przepisów w zakresie ochrony danych osobowych

	● konsultuje zabezpieczenia odnoszące się do ochrony danych osobowych ● udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie ● współpracuje i pełni rolę punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem ● uczestniczy w analizie ryzyka ● konsultuje projekty i zmiany operacyjne ● monitoruje zmiany regulacyjne w zakresie danych osobowych
Właściciel procesu (zasobu informacyjnego) / **osoba zajmująca stanowisko kierownicze**	● określa zasady dostępu i postępowania z informacjami, których jest właścicielem ● identyfikuje i ocenia ryzyka oraz opracowuje plany postępowania z ryzykami ● realizuje zadania z zakresu ciągłości działania uczelni
Dział Teleinformatyczny / Administrator systemu	● wdraża i utrzymuje zabezpieczenia w środowisku IT ● stosuje zasady bezpieczeństwa odnoszące się do IT ● identyfikuje i podejmuje reakcję na incydenty IT ● realizuje zadania z zakresu ciągłości działania
Zespół bezpieczeństwa (Inspektor bezpieczeństwa informacji, Inspektor ochrony danych, Administrator systemu)	● zapewniają wsparcie i uczestniczą w procesie zarządzania ryzykiem ● realizują obsługę incydentów ● raportują w zakresie bezpieczeństwa informacji do rektora lub innych osób pełniących funkcje kierownicze
Wszyscy pracownicy	● stosują regulacje w zakresie akceptowanego użycia zasobów informacyjnych ● postępują z informacjami zgodnie z przypisaną klasyfikacją

IV. KLASYFIKOWANIE INFORMACJI

1. Wprowadza się zasadę klasyfikowania informacji przetwarzanych w uczelni wprowadzając następujący podział:

1) **INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY (klauzula: *Szczególnie chronione*)** - to takie, które ściśle chronimy, zwykle jest to informacja dostępna dla kierownictwa oraz osób przez nich upoważnionych. Utrata lub nieuprawnione udostępnienie takiej informacji prowadzi do znaczących konsekwencji finansowych, prawnych lub może wpłynąć na pozycję uczelni. Klasyfikując informację jako *szczególnie chronioną* należy zawsze wskazać odbiorców tej informacji.

2) **INFORMACJE WYMAGAJĄCE OCHRONY (klauzula: *Chronione*)** - są to informacje zwykle dostępne dla każdego pracownika lub współpracownika uczelni. Ujawnienie informacji ma ograniczony wpływ na bezpieczeństwo informacji.

3) **INFORMACJE NIEWYMAGAJĄCE OCHRONY (klauzula: *Jawne*) -** to takie, których ujawnienie nie ma żadnego wpływu na bezpieczeństwo informacji jednak w niektórych sytuacjach informacja ta może wymagać ochrony przed utratą integralności i/lub dostępności.

2. Tworząc informacje (pliki, dokumenty, zbiory danych) lub będąc Właścicielem operacyjnym zasobu informacyjnego, równorzędnie ponosi się odpowiedzialność za sklasyfikowanie tej informacji.

3. Wszyscy pracownicy są odpowiedzialni za postępowanie z informacjami zgodnie z przyjętym schematem klasyfikacji informacji.

4. Szczegółowe wytyczne w zakresie klasyfikacji i postępowania z informacjami znajdują w Standardzie klasyfikacji informacji.

V. ZARZĄDZANIE RYZYKIEM

1. Działania w zakresie bezpieczeństwa informacji realizowane są w oparciu o proces zarządzania ryzykiem. Wynikiem tego procesu jest wdrożenie zabezpieczeń, które redukują ryzyko do akceptowalnego poziomu.

2. Ocenę ryzyka można podjąć w każdej sytuacji, gdy zmieniają się procesy lub otoczenie uczelni np. na skutek uruchomienia nowych projektów, wdrożenia istotnych zmian w systemach lub zmian regulacyjnych.

3. Proces zarządzania ryzykiem opisany jest szczegółowo w Standardzie zarządzania ryzykiem bezpieczeństwa informacji.

VI. PODSTAWOWE ZASADY OCHRONY

1. Planując i wdrażając ochronę informacji stosuje się następujące zasady:

1) **zasada minimalizacji uprawnień** – pracownik otrzymuje niezbędne uprawnienia, aby mógł wykonywać swoje zadania i obowiązki; uprawnienia te będą ograniczać dostęp do systemów, usług oraz danych;

2) **zasada wiedzy koniecznej** – przekazuje się informację ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych zadań;

3) **zasada ubezpieczania zabezpieczeń** – tam, gdzie to możliwe i efektywne, uczelnia będzie stosować zabezpieczenia wielowarstwowe, które wzajemnie się ubezpieczają;

4) **zasada indywidualnej odpowiedzialności** - odpowiedzialność za bezpieczeństwo poszczególnych elementów przypisuje się konkretnym osobom.

VII. MONITOROWANIE DZIAŁAŃ

Informuję, że wszelkie działania wykonywane w systemach teleinformatycznych należących do AB mogą być monitorowane. Zastrzegamy sobie prawo do ich wglądu i monitorowania z zachowaniem pełnej dbałości o ich poufność i integralność. Monitoring pozwoli nam tworzyć raporty, poprawiać bezpieczeństwo i unikać problemów technicznych. Dane z monitoringu mogą stanowić dowód w sprawie o naruszenie bezpieczeństwa informacji.

VIII. ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI

1. Zobowiązuje się wszystkich pracowników i współpracowników uczelni do zachowania poufności. Obowiązek zachowania poufności trwa również po ustaniu stosunku pracy lub innego stosunku prawnego, na podstawie którego była wykonywana praca na rzecz uczelni.

2. Wprowadza się zasadę potwierdzenia stosowania się do zachowania poufności przez podpisanie “Oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa Informacji oraz zachowaniu poufności (NDA)” - Załączniku nr 2.

3. Zasada zachowania poufności obowiązuje też podmioty zewnętrzne, co jest każdorazowo regulowane w ramach zawieranych umów.

IX. REAGOWANIE NA INCYDENTY

1. Wprowadza się zasadę zgłaszania wszelkich zidentyfikowanych nieprawidłowości lub zdarzeń, które mogą mieć wpływ na bezpieczeństwo informacji. Jeżeli pracownik posiada wiedzę lub podejrzewa, że dana sytuacja nosi znamiona naruszenia bezpieczeństwa lub incydentu, powinien zgłosić to bez zbędnej zwłoki.

2. Uczelnia zapewnia skuteczny model zarządzania incydentami, który opiera się na zasadach współpracy zespołowej. Zasady zarządzania incydentami zostały określone w Standardzie zarządzania incydentami.

X. ODSTĘPSTWA

Wszelkie odstępstwa od stosowania zasad Polityki oraz dokumentów powiązanych muszą zostać zgłoszone i zaakceptowane przez Zespół bezpieczeństwa, a w wyjątkowych przypadkach przez rektora lub inną wyznaczoną osobę pełniącą funkcję kierowniczą.

XI. EGZEKWOWANIE ZASAD BEZPIECZEŃSTWA

Uczelnia będzie dążyć do egzekwowania zasad bezpieczeństwa określonych niniejszą Polityką. Zastrzega się, że nieprzestrzeganie zasad wynikających z Polityki oraz dokumentów powiązanych może prowadzić do podjęcia właściwych sankcji dyscyplinarnych lub umownych na podstawie stosowanych przepisów prawa.

XII. DOSKONALENIE

1. Wprowadza się zasadę okresowego przeglądu skuteczności działania Polityki bezpieczeństwa oraz innych dokumentów związanych z bezpieczeństwem informacji.
2. Efektem przeglądu może być zaplanowanie i wdrożenie działań, które poprawią skuteczność zarządzania bezpieczeństwem informacji.
3. Niezależnie od wyników przeglądu Polityka oraz dokumenty zależne mogą się zmienić, zawsze, gdy:
    1) zidentyfikowane zostaną nowe ryzyka,
    2) zmienią się przepisy prawa lub regulacje wewnętrzne,
    3) nastąpią zmiany organizacyjne lub procesowe,
    4) będzie to wymagane w związku z przeglądami lub audytami bezpieczeństwa.
4. Zasady monitorowania, przeglądów i doskonalenia systemu zarządzania bezpieczeństwem informacji uczelni opisuje Standard nadzoru.