

**POLITYKA BEZPIECZEŃSTWA INFORMACJI**  
**W VIAMODA SZKOLE WYŻSZEJ W WARSZAWIE**

**§ 1.**

1. Celem Polityki Bezpieczeństwa Informacji (zwanej dalej „Polityką”) jest ustanowienie zasad oraz środków organizacyjnych, technicznych i fizycznych zapewniających ochronę informacji przetwarzanych w VIAMODA Szkole Wyższej W Warszawie (zwanej dalej „Uczelnią”).
2. Polityka obowiązuje wszystkich wykładowców, studentów, pracowników administracji, współpracowników, a także podmioty przetwarzające informacje na zlecenie Uczelni.
3. Pracownicy i studenci zobowiązani są do stosowania się do Polityki, zabezpieczania nośników i urządzeń oraz zgłaszania incydentów bezpieczeństwa.

**§ 2.**

Uczelnia zapewnia poufność informacji, integralność danych i dostępność systemów.

**§ 3.**

Podstawowe zasady Polityki bezpieczeństwa informacji w Uczelni to:

- 1) minimalizacja zbieranych danych;
- 2) dostęp do informacji tylko dla osób uprawnionych;
- 3) bezpieczne udostępnianie materiałów dydaktycznych;
- 4) ochrona plików projektowych, cyfrowych portfolio, prac artystycznych.

**§ 4.**

Nadzór nad prawidłowym działaniem Polityki sprawuje Kanclerz poprzez powołanych do tego celu pracowników:

- 1) Pełnomocnika Kanclerza ds. bezpieczeństwa informacji:
  - odpowiada za wdrożenie Polityki;
  - przeprowadza coroczny przegląd bezpieczeństwa informacji w Uczelni,
  - formułuje wnioski z audytu do wdrożenia;
  - nadzoruje przestrzeganie przepisów o ochronie danych osobowych,
  - przyjmuje zgłoszenia przypadków naruszenia bezpieczeństwa informacji;
- 2) Administratora systemów IT:
  - zabezpiecza systemy informacyjne Uczelni,
  - zarządza dostęпами,
  - tworzy kopie zapasowe.

**§ 5.**

Rozróżnia się następujące kategorie informacji:

- 1) publiczne – informacje dostępne dla każdego, np. ogłoszenia, organizacja roku akademickiego, zasady przyznawania pomocy materialnej itp.;
- 2) wewnętrzne – informacje dostępne tylko dla społeczności Uczelni (studenci, pracownicy);
- 3) poufne:
  - dane osobowe studentów i pracowników,
  - dokumentacja zaliczeniowa i egzaminacyjna,
  - dane finansowe,
  - dokumentacja Biura Obsługi Studenta.
- 4) ściśle poufne – dane dostępne do systemów.

#### **§ 6.**

1. Uprawnienia nadawane są pracownikom i studentom zgodnie z zasadą minimalnych uprawnień.
2. Uprawnienia do systemów nadaje:
  - 1) poczta elektroniczna – administrator systemów IT;
  - 2) MS Teams – uprawniony pracownik BOS w porozumieniu z administratorem systemów IT;
  - 3) POLON – administrator systemu POLON.
3. Po zakończeniu współpracy, skreśleniu z listy studentów konta są dezaktywowane.

#### **§ 7.**

1. Wszystkie pomieszczenia w których znajdują się dokumenty lub sprzęty dydaktyczne są chronione poprzez:
  - 1) dostęp tylko dla osób uprawnionych;
  - 2) obowiązek zamykania pomieszczeń;
  - 3) obowiązek zamykania dokumentów w szafach.
2. Systemy informatyczne są chronione hasłami wg zasad:
  - 1) min. 8 znaków;
  - 2) duże i małe litery, cyfry, znaki specjalne;
  - 3) zakaz używania tego samego hasła w prywatnych systemach.
3. Sieć jest chroniona wg zasad:
  - 1) sieci Wi-Fi zabezpieczone WPA3;
  - 2) dostęp do sieci administracyjnej tylko dla pracowników,
  - 3) obowiązkowe stosowanie VPN poza siecią kampusu.

#### **§ 8.**

1. Zasady pracy zdalnej i MS Teams:
  - 1) zasady pracy zdalnej
    - używanie urządzeń zabezpieczonych hasłem i antywirusem;
    - połączenie wyłącznie przez VPN (jeśli dotyczy systemów administracyjnych);
    - nieudostępnianie ekranu osobom postronnym;

- brak możliwości pracy na publicznych komputerach.
- 2) MS Teams
- wykorzystywany do zajęć online i konsultacji;
  - zakaz nagrywania zajęć bez zgody prowadzącego i studentów;
  - materiały dydaktyczne nie mogą być udostępniane poza Uczelnię;
  - obowiązkowe jest używanie kont uczelnianych.
2. Zasady korzystania z poczty i Internetu:
- 1) poczta e-mail;
- komunikacja dydaktyczna i organizacyjna odbywa się wyłącznie przez pocztę z domeną Uczelni;
  - zakaz otwierania podejrzanych załączników.
- 2) przy korzystaniu z Internetu zakazane jest:
- pobieranie nielegalnych materiałów;
  - instalowanie niesprawdzonego oprogramowania;
  - udostępnianie treści naruszających prawa autorskie.

#### **§ 9.**

1. W przypadku naruszenia bezpieczeństwa informacji należy niezwłocznie zgłosić ten fakt Kanclerzowi.
2. Przykłady naruszenia bezpieczeństwa informacji:
  - 1) utrata laptopa lub telefonu;
  - 2) nieuprawniony dostęp do systemu;
  - 3) wyciek danych osobowych;
  - 4) wirusy, phishing;
  - 5) uszkodzenie prac studentów i zasobów online.

#### **§ 10.**

Nieprzestrzeganie zasad może skutkować odpowiedzialnością dyscyplinarną lub porządkową.

#### **§ 11.**

W sprawach nieuregulowanych w niniejszej Polityce stosuje się odpowiednio przepisy prawa powszechnie obowiązującego.