POLITECHNIKA BIAŁOSTOCKA
WYDZIAŁ BUDOWNICTWA I NAUK O ŚRODOWISKU
15-351 Białystok, ul. Wiejska 45E
(+48) 85 746 95 60

POSTANOWIENIE NR 23/2026

Dziekana Wydziału Budownictwa i Nauk o Środowisku

Politechniki Białostockiej

z dnia 22.06. 2026 r.

w sprawie zwiększenia poziomu bezpieczeństwa systemu cyberbezpieczeństwa (KSC)

na Wydziale Budownictwa i Nauk o Środowisku

1. Zobowiązuję Dyrektorów Instytutów, Prodziekanów, Kierowników Katedr i Przewodniczącą Rady Naukowej Wydziału do stosowania wytycznych zawartych w Rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 28 kwietnia 2026 r., a w szczególności:

Rekrutacja i wdrożenie do pracy

Weryfikacja kandydatów

• Prowadzić rozmowy z włączoną kamerą. Zwracać uwagę na nienaturalne pauzy, opóźnienia, wyciszenia dźwięku w momentach, gdy kandydat powinien mówić.

• Przy podwyższonym ryzyku lub podejrzeniu nadużycia uwzględnić analizę dostępnych danych telemetrycznych i diagnostycznych połączenia, realizowaną przez uprawnionych administratorów.

• Potwierdzać historię zatrudnienia bezpośrednio u poprzednich pracodawców, a nie tylko na podstawie CV i profilu LinkedIn.

• Przy rolach o podwyższonym ryzyku rozważyć weryfikację tożsamości na żywo.

Pierwsze tygodnie pracy

• Poprosić pracownika o odczytanie numeru seryjnego urządzenia, co potwierdza fizyczny dostęp do sprzętu.

• Monitorować aktywność użytkownika pod kątem nietypowych godzin pracy.

• Nadawać uprawnienia stopniowo (least privilege). Monitorować próby eskalacji.

Po wykryciu podejrzenia lub incydentu

• Niezwłocznie zablokować konto i dostęp do wszystkich systemów.

• Przeprowadzić analizę zachowania użytkownika: historię logowań, używane narzędzia, ostatnie działania na repozytoriach i w systemach.

• Skontaktować się z właściwym zespołem reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego (CISRT NASK, CSIRT GOV, CSIRT MON) właściwym CSIRTem sektorowym, żeby skonsultować sytuację i zlecić jej dalszą analizę.

Spotkania wideo i linki

• Weryfikować domeny linków do spotkań. Prawidłowe adresy dla popularnych narzędzi do wideokonferencji, takich jak Zoom i Teams, to odpowiednio zoom.us i teams.microsoft.com.

Każda inna domena (np. teamslivc[.]com, ms-meet[.]xyz, micrusoft[.]us) stanowi sygnał ostrzegawczy.

• Nie pobierać plików ani nie uruchamiać poleceń terminalowych sugerowanych przez interfejs spotkania lub rozmówcę w trakcie połączenia wideo.

• Jeśli podczas spotkania wystąpią „problemy z dźwiękiem" i rozmówca proponuje „aktualizację" lub „naprawę" wymagającą pobrania pliku lub wklejenia komendy, należy natychmiast przerwać połączenie.

• Uwrażliwiać pracowników, że atakujący mogą kontaktować się z przejętych kont osób, które ofiara zna. Sam fakt, że wiadomość pochodzi od znanego kontaktu, nie oznacza, że jest bezpieczna.

• Zgłaszać podejrzane domeny i linki do właściwego CSIRT poziomu krajowego lub CSIRT sektorowego (jeśli został już ustanowiony w danym sektorze).

Konferencje i relacje biznesowe

• Kontakty nawiązane osobiście na konferencjach nie są automatycznie wiarygodne. Należy weryfikować firmy i osoby, które proponują współpracę techniczną lub integrację z systemami.

• Nie otwierać projektów z nieznanych repozytoriów bez wcześniejszej analizy.

• Nie instalować aplikacji dystrybuowanych poza oficjalnymi kanałami, na prośbę nowopoznanych kontaktów biznesowych.

• Zachować ostrożność wobec nowych partnerów, którzy szybko budują wiarygodność przez wpłaty własnych środków lub formalne procesy onboardingowe.

• Ograniczyć dostęp do repozytoriów i systemów wewnętrznych dla partnerów zewnętrznych. Stosować zasadę minimalnych uprawnień również wobec kontrahentów.

Ochrona pracowników technicznych i badaczy

• Informować pracowników technicznych (programistów, analityków bezpieczeństwa, badaczy) o tym, że są potencjalnymi celami spersonalizowanych kampanii rekrutacyjnych. Oferty pracy mogą być generowane przez AI na podstawie ich publikacji i aktywności online.

• Traktować z ostrożnością niezamówione oferty pracy, szczególnie jeśli: pochodzą z adresów darmowych skrzynek, odwołują się do firm, których nie można zweryfikować w publicznych źródłach lub kierują na strony zarejestrowane w ostatnich dniach.

• Weryfikować tożsamość osób proponujących współpracę badawczą, szczególnie jeśli propozycja wiąże się z uruchomieniem kodu, zainstalowaniem narzędzi.

• Rozważyć stosowanie izolowanych środowisk do analizy nieznanych projektów i narzędzi otrzymanych od osób spoza organizacji.

2. Powołuję Zespół do kontroli stosowania Rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa na Wydziale:

    1. mgr Bartosz Mikołajczyk
    2. mgr inż. Honorata Mrozek
    3. mgr Katarzyna Zgudko-Perkowska

DZIEKAN
WYDZIAŁU BUDOWNICTWA I NAUK O ŚRODOWISKU
Politechniki Białostockiej
prof. dr hab. inż. Michał Bołtryk