Zarządzenie nr 6/2026
Dyrektora Wojewódzkiego Ośrodka Animacji Kultury w Toruniu
z dnia 30 kwietnia 2026 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Systemów Informatycznych w Wojewódzkim Ośrodku Animacji Kultury w Toruniu

Działając na podstawie Ustawy z dnia 25.10.1991 (Dz. Ustaw 2012 POZ. 406 z późn. zm.) o organizowaniu i prowadzeniu działalności kulturalnej, zarządza się, co następuje:

§ 1.

Ustala się Politykę Bezpieczeństwa Informacji oraz Systemów Informatycznych Wojewódzkiego Ośrodka Animacji Kultury w Toruniu, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

1. Wykonanie zarządzenia zleca się osobie zatrudnionej na stanowisku specjalistki ds. obsługi sekretariatu i gościnności oraz specjaliście ds. informatyki w zakresie technicznym.
2. Osoba zatrudniona w sekretariacie zobowiązuje się do wyłożenia treści Polityki w dniu dzisiejszym w sekretariacie Wojewódzkiego Ośrodka Animacji Kultury przy ul. Kościuszki 75-77 do wglądu ogółu pracowników.
3. Treść Polityki zostanie przesłana drogą elektroniczną do wszystkich pracowników instytucji poprzez wewnętrzny komunikator (google chat).

§ 3.

1. Każdy pracownik Ośrodka jest zobowiązany do zapoznania się z treścią Polityki Bezpieczeństwa Informacji oraz Systemów Informatycznych.
2. Fakt zapoznania się z dokumentem pracownicy potwierdzają własnoręcznym podpisem na liście stanowiącej załącznik do polityki bezpieczeństwa

§ 4.

Zarządzenie wchodzi w życie z dniem 1 maja 2026

Dyrektor: Łukasz Wudarski

Łukasz Wudarski 2026.04.30 11:23:12 +02'00'

Załącznik do zarządzenia nr 6/2026 z dnia 30.04.2026

POLITYKA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW IT

Wersja: 2.0
Data wejścia w życie: 1 maja 2026 r.

---

1. Postanowienia ogólne

Niniejszy dokument określa zasady ochrony zasobów informacyjnych, sprzętu oraz danych osobowych w **Wojewódzkim Ośrodku Animacji Kultury w Toruniu**.
Celem polityki jest minimalizacja ryzyka wycieku danych, infekcji systemów oraz zapewnienie ciągłości działania instytucji.

Ważne: Każdy pracownik i współpracownik jest zobowiązany do przestrzegania niniejszych zasad. Nieznajomość polityki nie zwalnia z odpowiedzialności.

---

2. Zarządzanie dostępem i tożsamością

Bezpieczeństwo zaczyna się od logowania. W firmie obowiązują następujące standardy:

- **Zasada minimalnych uprawnień:** Pracownik ma dostęp tylko do tych danych, które są mu niezbędne do wykonywania pracy.
- **Polityka haseł:** * **8-12 znaków** (preferowane hasła tworzone i uaktualniane przez dział IT)
    - Musi zawierać wielkie litery, cyfry oraz znaki specjalne.
    - Zakaz używania tego samego hasła do kont prywatnych i służbowych.
- **MFA (Uwierzytelnianie dwuskładnikowe):** Jest obowiązkowe dla wszystkich kluczowych usług.
- **Blokowanie ekranu:** Każdorazowe odejście od biurka/komputera wymaga zablokowania stacji roboczej (skrót `Win + L` lub `Cmd + Ctrl + Q`).

---

3. Bezpieczeństwo fizyczne i sprzętowe

Sprzęt firmowy jest narzędziem pracy i podlega szczególnej ochronie:

- **Zasada "Czystego biurka":** Po zakończeniu pracy dokumenty papierowe zawierające dane poufne muszą zostać zamknięte w szafkach, a biurko uprzątnięte.
- **Nośniki zewnętrzne:** Zabrania się podłączania prywatnych pendrive'ów lub dysków do komputerów firmowych bez zgody działu IT.
- **Przechowywanie sprzętu:** Zabrania się pozostawiania laptopów służbowych w samochodach oraz miejscach publicznych bez nadzoru.

---

4. Praca zdalna i hybrydowa

Praca poza biurem nie zwalnia z czujności:

- **Publiczne Wi-Fi:** Kategoryczny zakaz logowania się do systemów firmowych przez otwarte, publiczne sieci Wi-Fi (np. w kawiarniach) bez użycia **VPN**.
- **Otoczenie:** Pracownik ma obowiązek dbać o to, aby osoby postronne (w tym domownicy) nie miały wglądu w ekran komputera lub dokumenty służbowe.

---

5. Ochrona danych osobowych (RODO)

Zgodnie z obowiązującymi przepisami:

1. Dane osobowe przetwarzane są wyłącznie w celach biznesowych.
2. Zabrania się kopiowania baz danych klientów na prywatne urządzenia lub chmury osobiste.
3. Utylizacja dokumentów papierowych musi odbywać się wyłącznie za pomocą niszczarek o odpowiednim standardzie bezpieczeństwa.

---

6. Procedura reagowania na incydenty

W przypadku podejrzenia naruszenia bezpieczeństwa (np. zgubienie laptopa, otrzymanie podejrzanego e-maila, wyciek danych), pracownik jest zobowiązany:

1. **Niezwłocznie zgłosić zdarzenie** do Inspektora Ochrony Danych lub Administratora Systemów Informatycznych/Specjalisty ds. Informatyki
2. Odłączyć zainfekowane urządzenie od sieci (Wi-Fi/Kabel).
3. Nie podejmować prób naprawy na własną rękę, aby nie zniszczyć logów systemowych.

---

7. Zasady korzystania z narzędzi Sztucznej Inteligencji (AI)

W celu zachowania poufności danych przy jednoczesnym wspieraniu innowacyjności, wprowadza się następujące zasady korzystania z narzędzi AI:

Zakaz wprowadzania danych poufnych: Surowo zabrania się wpisywania do publicznych czatów AI danych osobowych klientów, pracowników, kodów źródłowych oprogramowania firmy, strategii biznesowych oraz szczegółów finansowych.

Weryfikacja merytoryczna: Modele AI mogą generować nieprawdziwe informacje (tzw. halucynacje). Pracownik ma obowiązek każdorazowo zweryfikować wynik pracy AI przed jego wykorzystaniem w procesach decyzyjnych lub komunikacji z klientem.

Prawa autorskie i licencje: Przed wykorzystaniem treści wygenerowanych przez AI w celach komercyjnych (np. grafiki, teksty marketingowe), pracownik musi upewnić się, że licencja danego narzędzia na to pozwala i nie narusza praw osób trzecich.

Zatwierdzone narzędzia: Zaleca się korzystanie wyłącznie z płatnych narzędzi AI w wersjach Gemini oraz ChatGPT zakupionych przez WOAK, które gwarantują, że wprowadzane dane nie są wykorzystywane do trenowania modeli publicznych.

---

8. Bezpieczeństwo urządzeń mobilnych (smartfony i tablety)

Urządzenia mobilne używane do celów służbowych (zarówno firmowe, jak i prywatne używane do celów służbowych) muszą spełniać najwyższe standardy ochrony:

Zabezpieczenia biometryczne i PIN (wymuszone automatycznie przez Workspace): Każde urządzenie musi być chronione silnym kodem blokady (minimum 6 cyfr) lub uwierzytelnianiem

biometrycznym (odcisk palca, skan twarzy). Zabrania się używania prostych wzorów graficznych („wężyków”).

Zabezpieczenie dostępu zdalnego: Zaleca się dodanie konta administracyjnego WOAK, które w razie utraty urządzenia (awaria, kradzież) pomoże odzyskać dane i zdalnie zablokować dostęp do nich.

Zdalne czyszczenie danych: W przypadku zgubienia lub kradzieży urządzenia, pracownik ma obowiązek natychmiast zgłosić ten fakt działowi IT, aby umożliwić zdalne wykasowanie danych firmowych.

Aktualizacje systemu: Pracownik jest zobowiązany do regularnego instalowania aktualizacji systemu operacyjnego (iOS/Android) oraz aplikacji.

Zaufane źródła aplikacji: Surowo zabrania się instalowania aplikacji spoza oficjalnych sklepów (App Store / Google Play) oraz dokonywania modyfikacji systemu typu Jailbreak lub Rooting, które zdejmują fabryczne zabezpieczenia producenta.

Oddzielenie danych: Zaleca się (a w przypadku urządzeń firmowych wymaga), aby aplikacje służbowe (e-mail, Chat, Dysk Google) były oddzielone od prywatnych. Zabrania się używania służbowego smartfona przez osoby trzecie (np. udostępnianie dziecku do gier).

---

9. Sankcje

Oznaczanie treści: W przypadku generowania dokumentów lub grafik w całości przez AI, zaleca się (jeśli wymaga tego polityka konkretnego działu) dodanie adnotacji: "Treść wygenerowana/wspomagana przez sztuczną inteligencję".

Naruszenie zasad niniejszej polityki może być traktowane jako ciężkie naruszenie obowiązków pracowniczych i skutkować karami porządkowymi, rozwiązaniem umowy o pracę lub odpowiedzialnością cywilno-prawną.
