ZARZĄDZENIE NR 10/2026
z dnia 02 kwietnia 2026 r.
Dyrektora Medycznej Szkoły Policealnej
im. Hanny Chrzanowskiej w Otwocku.

w sprawie wdrożenia Regulaminu Bezpieczeństwa Informacji w Medycznej Szkole Policealnej im. Hanny Chrzanowskiej w Otwocku.

Na podstawie 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 §7 ust. 1 pkt 7 Statutu Medycznej Szkoły Policealnej im. Hanny Chrzanowskiej w Otwocku, wprowadzonego uchwałą Rady Pedagogicznej nr 6/2023 z dnia 27 maja 2023 r. z późn. zm., zarządzam, co następuje:

§1.

Wprowadza się Regulamin Bezpieczeństwa Informacji w Medycznej Szkole Policealnej im. Hanny Chrzanowskiej w Otwocku, który stanowi załącznik do niniejszego Zarządzenia.

§2.

Zobowiązuje się wszystkich pracowników Medycznej Szkoły Policealnej im. Hanny Chrzanowskiej w Otwocku do zapoznania się i stosowania procedur określonych w Regulaminie Bezpieczeństwa Informacji w Medycznej Szkole Policealnej Im. Hanny Chrzanowskiej w Otwocku.

§3.

Wykonanie Zarządzenia powierza się administratorowi sieci komputerowej, który jest odpowiedzialny za prawidłową realizację procedur zawartych w Regulaminie Bezpieczeństwa Informacji w Medycznej Szkole Policealnej im. Hanny Chrzanowskiej w Otwocku.

§4.

Zarządzenie wchodzi w życie z dniem podjęcia.

Dyrektor
Żaneta Kuczewska

Załącznik do Zarządzenia nr 10/2026
z dnia 02 kwietnia 2026 r.

REGULAMIN BEZPIECZEŃSTWA INFORMACJI W MEDYCZNEJ SZKOLE POLICEALNEJ IM. HANNY CHRZANOWSKIEJ W OTWOCKU

I. Wprowadzenie

1. Regulamin Bezpieczeństwa Informacji w Medycznej Szkole Policealnej im. Hanny Chrzanowskiej w Otwocku (zwany dalej „Regulaminem") określa zasady ochrony danych osobowych w Medycznej Szkole Policealnej im. Hanny Chrzanowskiej w Otwocku i jest wprowadzany w związku z przepisami rozporządzenia PEiR (UE) nr 2016/679 z 27.04.2016 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 (Dz. Urz. UE L z 2016 r. 119, s. 1 ze zm.) – dalej „RODO".
2. W Regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji w Medycznej Szkole Policealnej im. Hanny Chrzanowskiej w Otwocku (zwanej dalej „Administratorem").

II. Zasady przetwarzania danych osobowych

1. Każdy pracownik Administratora przetwarza dane osobowe wyłącznie w związku z wykonywaniem swoich zadań służbowych. Pracownicy są zobowiązani do **zachowania poufności** danych osobowych i ich zabezpieczeń. Udostępnianie danych osobom trzecim jest zabronione.
2. W przypadku uzyskania przez pracownika dostępu do danych osobowych (papierowych lub elektronicznych) przekraczających zakres upoważnienia tego pracownika, udostępnione w ten sposób informacje należy zachować w poufności. Należy również poinformować pracownika odpowiedzialnego za udostępnione dokumenty o zaistniałej sytuacji, a także zawiadomić Inspektora Ochrony Danych o incydencie.
3. Pracownik jest obowiązany **logować się do systemu za pomocą własnego loginu oraz hasła** dostępu. Udzielanie informacji na temat loginu i hasła innym osobom jest zabronione.
4. Pracownik ma prawo korzystać z Internetu wyłącznie w celu wykonywania obowiązków służbowych, **zabronione jest korzystanie z prywatnej poczty służbowej, prywatnych profili na social mediach**, wykorzystywanie komercyjnych komunikatorów **typu WhatsApp** oraz korzystanie **z ogólnie dostępnej wersji Chata GPT przy realizacji obowiązków służbowych**.
5. Pracownicy zobowiązani są do **przechowywania na biurku tylko tych dokumentów, które są im niezbędne** w danym momencie do wykonania bieżących zadań.

6. Opuszczając czasowo stanowisko pracy pracownik ma obowiązek zablokować komputer poprzez wylogowanie się z programu oraz dokonać blokady systemu operacyjnego, za pomocą skrótu klawiszowego **[Windows + L]** lub **[Cmd + Ctrl + Q]** – w zależności od systemu operacyjnego komputera.
7. Kończąc pracę pracownik pozostaje przy stanowisku komputerowym do czasu **całkowitego wyłączenia się komputera**.
8. Po zakończonej pracy pracownik jest zobowiązany do wylogowania się z systemu. Na biurku może pozostać jedynie telefon oraz materiały biurowe, takie jak np. długopis i zszywacz – **zasada czystego biurka**.
9. Po pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy/szafki. Klucze do szaf należy umieścić w wyznaczonym do tego celu umówionym, bezpiecznym miejscu.
10. Obowiązuje zakaz trzymania na biurku wszelkich produktów spożywczych, których posiadanie grozi rozlaniem płynu.
11. **Zabronione** jest korzystanie z **prywatnych nośników informacji** (np. dysk zewnętrzny, pendrive).
12. **Zabronione** jest korzystanie ze sprzętu prywatnego, tj. telefon, tablet, laptop.
13. Korzystając ze **służbowych nośników pamięci (np. pendrive)** bezwzględnie wymagane jest ich **zaszyfrowania odpowiednim hasłem dostępu**.
14. Bez potrzeby nie należy tworzyć plików komputerowych zawierających dane osobowe. Pliki z danymi po ustaniu przydatności należy trwale **usunąć.**
15. Wszelkie dokumenty zawierające dane osobowe należy niszczyć **za pomocą niszczarek** dokumentów- **zasada czystego kosza**.
16. Pliki z dany osobowymi (Word, Excel, PDF, 7zip,) przed wysłaniem za pośrednictwem komunikacji elektronicznej powinny być **zaszyfrowane,** a hasło powinno być wysłane oddzielnym kanałem komunikacji (np. sms).
17. Pracownicy zobowiązani są do tworzenia **silnych haseł** do plików, poczty i systemów zgodnie z polityką haseł przyjętą u Administratora.
18. **Zabronione jest otwieranie załączników i klikanie w linki** pochodzące od nieznanych nadawców bądź podejrzane, sugerujące próbę phishingową. Podejrzane e-maile należy zgłaszać niezwłocznie wyznaczonemu Inspektorowi Ochrony Danych.
19. Wysyłając e-mail do wielu odbiorców spoza organizacji, pamiętamy o użyciu funkcji UDW.
20. Każdy pracownik jest odpowiedzialny za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe i **nie pozostawianie wydruków z danymi osobowymi na drukarce – zasad czystego druku**.
21. Zabronione jest **samodzielne instalowanie i pobieranie programów** przez pracowników.
22. Pracownicy zobowiązani są do przenoszenia dokumentów i sprzętu służbowego w sposób zapobiegający ich kradzieży, zagubieniu lub utracie, odpowiadając za ich zabezpieczenie.
23. Pracownicy są obowiązani do przekazywania Administratorowi nośników z danymi przeznaczonych do **zniszczenia**.
24. Pracownicy zobowiązani są do ustawienia wygaszaczy ekranu, uruchamiających blokadę systemu po **5 minutach bezczynności**.
25. Pracownicy zobowiązani są prowadzić swoją aktywności w prywatnych mediach społecznościowych **przy zachowaniu dbałości o dobre imię pracodawcy, jego wizerunek czy ochronę tajemnicy przedsiębiorstwa** w ramach przysługujących im praw i obowiązków pracowniczych, nie naruszając przepisów art. 212 §1 i § 2 KK.

26. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym.

ZGŁASZANIE INCYDENTÓW W ZAKRESIE DANYCH OSOBOWYCH

Pracownik zobowiązany jest do **NIEZWŁOCZNEGO** powiadomienia Inspektora Ochrony Danych – e-mail: iod@odokancelaria.pl, **tel. 577 940 399** w przypadku **stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych,** np. ślady na drzwiach, oknach i szafach wskazują na próbę włamania; niszczenie dokumentacji bez użycia niszczarki; wysyłka maila z niezaszyfrowanym załącznikiem zawierającym dane osobowe, wysyłka maila na zewnątrz organizacji bez stosowania kopi UDW, omyłkowa wysyłka maila na inny adres, wynoszenie danych osobowych w wersji papierowej i elektronicznej poza siedzibę Administratora bez zgody przełożonego; otrzymanie maili zachęcających do ujawnienia identyfikatora i/lub hasła, udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej, korzystanie z niezaszyfrowanych dysków czy pendriv-ów.

Dyrektor
Żaneta Kuczewska