

**Załącznik  
do Zarządzenia nr 10/XVI R/2025**

**Rektora Uniwersytetu Medycznego we Wrocławiu**

**z dnia 28 stycznia 2025 r.**

**Egz. pojedynczy**

|  |
| --- |
| **Z A T W I E R D Z AM**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Rektor**  **Uniwersytetu Medycznego** |

**POLITYKA BEZPIECZNEŃSTWA INFORMACJI**

**Uniwersytetu Medycznego**

**im. Piastów Śląskich we Wrocławiu**

WROCŁAW

2025

**§1**

**Deklaracja o ustanowieniu Polityki Bezpieczeństwa Informacji w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu**

Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu (zwany dalej Uniwersytetem Medycznym) jest jednym z wiodących w kraju ośrodkiem kształcenia kadr medycznych   
o ugruntowanej pozycji, zajmującym się kształceniem lekarzy różnych specjalności oraz szeroko pojętego personelu medycznego (farmaceutów, pielęgniarek, położnych, fizjoterapeutów, menedżerów ochrony zdrowia i innych), uczestniczącym w działalności dydaktycznej, naukowej oraz sprawowaniu opieki medycznej realizowanej w szpitalach klinicznych. Współpracuje z wieloma partnerami w kraju i z zagranicy. Do realizacji swoich zadań Uniwersytet Medyczny wykorzystuje nowoczesne systemy teleinformatyczne, od sprawności i niezawodności których uzależnione jest jego niezakłócone funkcjonowanie.

Bezpieczeństwo informacji jest nie tylko normą i koniecznością, ale także obowiązkiem. Władze Uniwersytetu Medycznego dostrzegają zagrożenia związane z bezpieczeństwem informacji zarówno w systemach teleinformatycznych, jak również w formie papierowej   
i innej. Uznają obowiązek ochrony aktywów Uniwersytetu Medycznego, które mogą zostać narażone na utratę poufności, integralności i dostępności w trakcie ich przetwarzania lub przechowywania.

Rektor Uniwersytetu Medycznego wprowadzając Politykę Bezpieczeństwa Informacji (zwaną dalej PBI) deklaruje wsparcie dla jej realizacji, a także zapewnienie odpowiednich środków do jej wdrożenia.

**§2**

**Słownik terminów**

Występujące w PBI zwroty oznaczają:

**aktywa** – wszystko co ma wartość dla Uniwersytetu Medycznego;

**dostępność** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;

**poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom;

**integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów;

**bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji. Dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

**incydent związany z bezpieczeństwem informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działalności Uniwersytetu Medycznego i zagrażają bezpieczeństwu informacji;

**System Zarządzania Bezpieczeństwem Informacji (SZBI)** – to część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka instytucji, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

**§3**

**Regulacje ogólne**

1. Życie i zdrowie ludzi jest dobrem najwyższym i ich ochrona w sytuacji zagrożenia jest ważniejsza niż ochrona jakichkolwiek innych zasobów.
2. Celem ustanowienia PBI jest zapewnienie zachowania poufności, dostępności i integralności informacji przetwarzanych w Uniwersytecie Medycznym.
3. Ochronie podlegają wszystkie aktywa informacyjne Uniwersytetu Medycznego,   
   a w szczególności:

* informacje przetwarzane w Uniwersytecie Medycznym, niezależnie od ich formy nośnika;
* sprzęt wykorzystywany do przetwarzania, przesyłania i przechowywania informacji   
  w Uniwersytecie Medycznym;
* pomieszczenia, w których znajduje się kluczowy sprzęt informatyczny, dokumenty zawierające tajemnicę Uniwersytetu Medycznego;
* oprogramowanie wykorzystywane w systemach teleinformatycznych Uniwersytetu Medycznego;
* wizerunek Uniwersytetu Medycznego;
* zasoby archiwalne Uniwersytetu Medycznego;
* pozostałe mienie wykorzystywane przez Uniwersytet Medyczny lub będące jego własnością;
* informacje, których właścicielem są kontrahenci lub jednostki zewnętrzne współpracujące z Uniwersytetem Medycznym.

1. Bezpieczeństwo informacji Uniwersytetu Medycznego obejmuje nie tylko jego siedzibę, ale także wszelkie miejsca i sytuacje, w których informacje związane z działalnością Uniwersytetu Medycznego są przetwarzane poza jego siedzibą. Obejmuje to   
   w szczególności zdalny dostęp do sieci komputerowej Uniwersytetu Medycznego.

**§4**

**Zakres PBI**

PBI odnosi się do wszelkich zasobów, inaczej aktywów zaangażowanych pośrednio lub bezpośrednio w realizację procesów dydaktycznych, naukowych, klinicznych i biznesowych, w tym zwłaszcza aktywów informacyjnych, a także usług elektronicznych. PBI dotyczy wszystkich pracowników Uniwersytetu Medycznego, jak również doktorantów, stażystów, rezydentów, praktykantów, wolontariuszy, studentów, itp.,   
a także osób oraz innych instytucji współpracujących z Uniwersytetem Medycznym   
w jakikolwiek sposób. Dokument PBI ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przetwarzane i przechowywane (papierowej, elektronicznej i innej).

Niniejszy dokument jest najwyższy rangą w zakresie ochrony i bezpieczeństwa informacji   
w Uniwersytecie Medycznym. Jest dokumentem nadrzędnym w stosunku do polityk szczegółowych oraz pozostałych dokumentów dotyczących informacji przetwarzanych   
w Uniwersytecie, w szczególności takich jak: zarządzenia rektora w sprawie wprowadzenia Polityki ochrony danych osobowych Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, Instrukcji zarządzania siecią i systemami informatycznymi w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Regulaminu monitoringu wizyjnego w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Procedury fizycznego dostępu do pomieszczeń oraz dokumentów zawierających dane osobowe przechowywanych w wersji papierowej w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu oraz Procedury ochrony danych osobowych w badaniach naukowych prowadzonych w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu.

**§5**

**Cele i zasady bezpieczeństwa informacji**

1. **Cele Bezpieczeństwa Informacji w Uniwersytecie Medycznym**

Niezakłócona i bezpieczna realizacja zadań w dziedzinie dydaktycznej, naukowej, opiekuńczo - medycznej oraz biznesowej, zależy od zapewnienia bezpieczeństwa informacji i usług, i jest możliwa pod warunkiem zrealizowania poniższych celów oraz związanych z nimi strategii wyrażających potrzeby bezpieczeństwa Uniwersytetu Medycznego.

1. Cel 1: Należy zapewnić ciągłość i bezpieczeństwo realizacji procesów dydaktycznych, naukowych, opiekuńczo - medycznych i biznesowych przez:

* ograniczenie wpływu szeroko pojętych zagrożeń natury teleinformatycznej (tj. systemy, ludzie, organizacja);
* zapewnienie wysokiego poziomu niezawodności i dostępności usług oferowanych przez systemy;
* utrzymywanie wysokiego, adekwatnego do potrzeb Uniwersytetu Medycznego poziomu poufności, integralności i dostępności informacji, niezależnie od jej postaci.

1. Cel 2: Należy zapewnić działania zgodne z prawem poprzez:

* właściwą ochronę informacji zaliczanych do tajemnic prawnie chronionych;
* przestrzeganie istniejących aktów prawnych, w tym prawa autorskiego;
* właściwą ochronę informacji związanych z zawartymi umowami;
* świadczenie usług w formie elektronicznej zgodnie z obowiązującym prawem.

1. Cel 3: Należy zapewnić ochronę wizerunku i reputacji Uniwersytetu Medycznego przez:

* ograniczenie wpływu szeroko pojętych zagrożeń natury teleinformatycznej;
* ograniczenie wpływu zagrożeń dla realizacji zobowiązań wynikających z zawartych umów oraz z dobrych obyczajów.

Władze Uniwersytetu Medycznego wyrażają wsparcie oraz gotowość poniesienia kosztów dla osiągnięcia tych celów i utrzymywania wynikającego z nich poziomu bezpieczeństwa w Uniwersytecie Medycznym, jednak dobór środków i metod zabezpieczeń fizycznych, technicznych oraz administracyjnych powinien uwzględniać wyniki szczegółowych analiz bezpieczeństwa, szacowania ryzyka oraz aspekt ekonomiczny.

1. Skuteczna ochrona zasobów informacyjnych Uniwersytetu Medycznego wymaga wspólnego działania i zaangażowania wszystkich pracowników, a także studentów   
   i doktorantów.
2. Obowiązek ochrony zasobów Uniwersytetu Medycznego, w przypadku współpracy z kontrahentami i jednostkami zewnętrznymi, określany jest w ramach umów zawartych z tymi podmiotami.
3. Pracownicy Uniwersytetu Medycznego zobowiązani są do używania zasobów informacyjnych Uniwersytetu Medycznego wyłącznie do celów służbowych, chyba, że regulacje szczegółowe stanowią inaczej. Wszelkie operacje wykonywane w sieci komputerowej Uczelni (z pocztą elektroniczną włącznie), w szczególności dotyczące zasobów wrażliwych pod względem poufności, mogą być monitorowane.
4. **Podstawowe zasady bezpieczeństwa informacji**

Poniższe uniwersalne zasady są podstawą dla stworzenia i utrzymania skutecznego Systemu Zarządzania Bezpieczeństwem Informacji:

1. Zasada uprawnionego dostępu – każdy pracownik przeszedł szkolenie i zapoznał się z PBI, akceptuje jej treść, podpisał oświadczenie o zapoznaniu się z PBI uzyskując możliwość dostępu do informacji.
2. Zasada przywilejów koniecznych – każdy pracownik posiada prawo dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
3. Zasada wiedzy koniecznej – każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań (zasada wiedzy uzasadnionej *need to know*).
4. Zasada usług koniecznych – udostępniane powinny być takie usługi, jakie są konieczne do realizacji zadań statutowych.
5. Zasada asekuracji – każdy mechanizm zabezpieczający musi być ubezpieczony innym (podobnym). W przypadkach szczególnych może być stosowane dodatkowe, trzecie niezależne zabezpieczenie.
6. Zasada świadomości zbiorowej – wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
7. Zasada indywidualnej odpowiedzialności – za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
8. Zasada obecności koniecznej – prawo przebywania w określonych miejscach i strefach mają tylko osoby upoważnione.
9. Zasada stałej gotowości – system jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
10. Zasada najsłabszego ogniwa – poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
11. Zasada kompletności – zabezpieczenie jest skuteczne tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
12. Zasada ewolucji – każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
13. Zasada odpowiedniości – używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.
14. Zasada świadomej konwersacji – nie zawsze i wszędzie trzeba mówić co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
15. Zasada segregacji zadań – zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła zdobyć pełni władzy nad całą organizacją (całym systemem).
16. Zasada prywatności kont w systemach– każdy pracownik i współpracownik Uniwersytetu Medycznego, a także każdy kto został dopuszczony do pracy   
    w systemach teleinformatycznych Uniwersytetu Medycznego, zobowiązany jest do pracy w tych systemach na przypisanych mu kontach jednoznacznie go identyfikujących i wyróżniających.

Do realizacji zadań służbowych należy korzystać wyłącznie ze służbowej poczty elektronicznej.

1. Zasada poufności haseł i kodów dostępu– każdy pracownik i współpracownik Uniwersytetu Medycznego zobowiązany jest do zachowania poufności i nie przekazywania innym osobom udostępnionych mu haseł i kodów dostępu,   
   w szczególności dotyczy to jego osobistych haseł dostępu do systemów teleinformatycznych i kodów dostępu do stref i pomieszczeń. Indywidualnego hasła nie należy przekazywać ani przełożonemu, ani administratorom, a jeśli do tego doszło, to należy je zmienić przy pierwszej okazji.
2. Zasada zamkniętego pomieszczenia– niedopuszczalne jest pozostawienie niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak   
   i po jej zakończeniu, jeśli nie pozostaje w nim osoba upoważniona. Zasada nie dotyczy pomieszczeń ogólnie dostępnych. Na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna   
   i drzwi oraz zabezpieczyć klucze do pomieszczenia, zgodnie z obowiązującymi zasadami nadzorowania kluczy.
3. Zasada czystego biurka– należy unikać pozostawiania bez nadzoru dokumentów na biurku. Po godzinach pracy wszystkie dokumenty stanowiące tajemnicę Uniwersytetu Medycznego i istotne dla niego muszą być przechowywane w zamkniętych szafkach, szufladach, regałach itp.
4. Zasada czystej tablicy– po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice (flipchart, wyłączyć rzutnik itp.).
5. Zasada czystego ekranu– każdy komputer musi mieć ustawiony, włączający się automatycznie wygaszacz ekranu. Dodatkowo przed pozostawieniem włączonego komputera bez opieki użytkownicy powinni zablokować go (włączając wygaszacz ekranu) lub w przypadku dłuższej nieobecności wylogować się z systemu.
6. Zasada czystych drukarek– informacje drukowane powinny być zabierane z drukarek natychmiast po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru.
7. Zasada czystego kosza– dokumenty papierowe i miękkie nośniki danych, z wyjątkiem materiałów jawnych, promocyjnych, marketingowych i informacyjnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie (w niszczarce, umieszczane w specjalnie przeznaczonych do tego celu pojemnikach itp.).
8. Zasada odpowiedzialności za zasoby- każdy użytkownik odpowiada za udostępnione mu zasoby (komputery, oprogramowanie, systemy, konta, karty dostępowe itp.).

**§6**

**Odpowiedzialność za bezpieczeństwo informacji   
w Uniwersytecie Medycznym**

Odpowiedzialność za bezpieczeństwo informacji w Uniwersytecie Medycznym ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Władze Uniwersytetu Medycznego są odpowiedzialne za zapewnienie warunków niezbędnych dla funkcjonowania   
i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Każdy pracownik Uniwersytetu Medycznego, jak również doktoranci, studenci, stażyści, rezydenci, praktykanci, wolontariusze itp. mają obowiązek zapoznania się z przedmiotowym dokumentem PBI. Kierownicy jednostek organizacyjnych są odpowiedzialni za bezpieczeństwo informacji w swojej jednostce organizacyjnej, a w szczególności za przestrzeganie zasad bezpieczeństwa przez podległy personel oraz podejmowanie odpowiednich działań w przypadku wystąpienia incydentu zagrożenia utraty bezpieczeństwa informacji.

1. **Rola i odpowiedzialność osób funkcyjnych**

W celu zapewnienia właściwej realizacji PBI w Uniwersytecie Medycznym oraz koordynacji wszystkich spraw w zakresie Systemu Zarządzania Bezpieczeństwem Informacji, w Uniwersytecie Medycznym funkcjonuje następująca struktura organizacyjna:

1. Kierownik Centrum Informatycznego jest odpowiedzialny za całokształt spraw związanych   
   z ochroną informacji w sieciach i systemach informatycznych;
2. Pełnomocnik Rektora ds. Ochrony Informacji Niejawnych jest odpowiedzialny za całokształt spraw związanych z ochroną informacji niejawnych;
3. Inspektor Ochrony Danych jest odpowiedzialny za informowanie władz i pracowników Uniwersytetu Medycznego o obowiązkach wynikających z powszechnie obowiązujących przepisów i wewnętrznych regulacji w zakresie ochrony danych osobowych oraz monitorowanie przestrzegania przepisów i wewnętrznych polityk regulujących przetwarzanie danych osobowych;
4. Rektor może powołać Zespół Bezpieczeństwa Informacji (zwany dalej „ZBI”), w którego skład w zależności od potrzeb mogą wchodzić w szczególności:

* Dyrektor Generalny lub wyznaczony Zastępca
* Specjalista ds. Obronnych, Obrony Cywilnej i Zarzadzania Kryzysowego
* Pełnomocnik Rektora ds. Ochrony Informacji Niejawnych
* Z-ca Dyr. Gen. ds. Komunikacji i PR Uczelni
* Kierownik Centrum Informatycznego
* Przedstawiciel Biura Rektora
* Pracownik Działu Zarzadzania Dokumentacją
* Pracownik Inspektoratu ds. BHP
* Specjalista ds. systemów bezpieczeństwa i ppoż.
* Inspektor Ochrony Danych
* Radca Prawny
* Audytor Wewnętrzny (z głosem doradczym)
* Inne osoby, których włączenie do Zespołu okaże się konieczne.

ZBI będzie odpowiedzialny za ocenę funkcjonowania mechanizmów bezpieczeństwa informacji w Uniwersytecie Medycznym i przedstawianie propozycji dokonania zmian w stosownych dokumentach, procedurach, infrastrukturze technicznej itp. oraz koordynowanie wdrażania i rozwoju Systemu Bezpieczeństwa Informacji. Szczegółowy zakres zadań ZBI określa Rektor w zarządzeniu o jego powołaniu.

1. **Sankcje za naruszenie zasad bezpieczeństwa informacji**

Nieprzestrzeganie zasad zawartych w dokumencie PBI jest naruszeniem obowiązków pracowniczych i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie sprawcy naruszenia do odpowiedzialności wynikającej z przepisów prawa powszechnie obowiązującego i Regulaminu Pracy Uniwersytetu Medycznego.

**§7**

**Wymagania dotyczące szkolenia**

1. Każdy pracownik, jak również doktorant, student, wolontariusz, stażysta, rezydent, praktykant Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu ma obowiązek zapoznania się z PBI.
2. Obowiązkiem Kierownika (bezpośredniego przełożonego) jest doprecyzowanie obowiązków wynikających z PBI na konkretnym stanowisku pracy.
3. Za zapoznanie z zapisami PBI osób oraz instytucji współpracujących z Uniwersytetem Medycznym odpowiedzialny jest pracownik Uniwersytetu Medycznego, który będzie tę współpracę organizował lub nadzorował.

**§8**

**Ochrona danych osobowych**

* + - 1. Przetwarzanie danych osobowych odbywa się zgodnie z powszechnie obowiązującymi przepisami prawa i wewnętrznymi politykami Uniwersytetu Medycznego.
  1. Szczegółowe zasady postępowania oraz stosowane środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa w obszarze ochrony danych osobowych zostały uregulowane w Zarządzeniu nr 93/XV R/2018 Rektora Uniwersytetu Medycznego we Wrocławiu z dnia 1 sierpnia 2018 r. **w sprawie wprowadzenia Polityki ochrony danych osobowych Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, Instrukcji zarządzania siecią i systemami informatycznymi w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Regulaminu monitoringu wizyjnego   
     w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, Procedury fizycznego dostępu do pomieszczeń oraz dokumentów zawierających dane osobowe przechowywanych w wersji papierowej w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu oraz Procedury ochrony danych osobowych w badaniach naukowych prowadzonych w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu**.

**§9**

**Rozpowszechnianie i zarządzanie dokumentem PBI**

Zaleca się rozpowszechnianie niniejszego dokumentu wśród pracowników Uniwersytetu Medycznego, jego partnerów, wybranych urzędów lub organów administracji publicznej, jako dowodu zwracania szczególnej uwagi na bezpieczeństwo informacyjne Uniwersytetu Medycznego i jego partnerów.

**§10**

**Zgodność z przepisami prawa**

W Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu ochrona informacji realizowana jest zgodnie z następującymi przepisami prawa, w szczególności:

* Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz.U. z 2024 r. poz. 1571 ze zm.);
* Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz.U. z 2024 r., poz. 799 ze zm.);
* Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U.   
  z 2023 r., poz. 2465 ze zm.) wraz z mającymi zastosowanie aktami wykonawczymi;
* Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U.   
  z 2024 r., poz. 581 ze zm.);
* Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t.j. Dz.U. z 2024 r., poz. 1061 ze zm.);
* Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (t.j. Dz.U. z 2024 r., poz. 17 ze zm.);
* Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz.U. z 2023 r., poz. 1465 ze zm.);
* Ustawa z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (t.j. Dz.U.   
  z 2024 r., poz. 572 ze zm.);
* Rozporządzenie 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);
* Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz.1781 ze zm.);
* Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2024 r., poz. 632 ze zm.);
* Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2022 r., poz. 1233 ze zm.);
* Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (t.j, Dz. U. z 2021 r., poz. 1995 ze zm.);
* Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz.U. z 2023, poz. 120 ze zm.);
* Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2025 r., poz. 24 ze zm.);
* Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r.,
* poz. 902 ze zm.);
* Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (t.j. Dz.U. z 2015 r., poz. 1341 ze zm.);
* Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (tj. Dz.U. z 2024 r., poz.1769  
  ze zm.);
* Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2024 r. poz. 1725 ze zm.);
* Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r. poz. 1557 ze zm.).

# **ZAŁĄCZNIKI**

**1. Załącznik 1 do PBI – Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, o zobowiązaniu do zachowania poufności.**

**2. Załącznik 1a do PBI – Oświadczenie Doktorantów Szkoły Doktorskiej o zapoznaniu się   
z Polityką Bezpieczeństwa Informacji w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu, o zobowiązaniu do zachowania poufności.**

**OPRACOWAŁ**

Pełnomocnik ds. Ochrony Informacji Niejawnych

Uniwersytetu Medycznego

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Wykonano w egz. pojedynczym

W.B. (tel. +48717841541)

**Załącznik 1 do PBI**

**Zarządzenie nr 10/XVI R/2025**

Wrocław, dn., \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

….....................................................................

**(imię i nazwisko)**

….....................................................................

**(jednostka organizacyjna)**

….....................................................................

…......................................................................

**(stanowisko służbowe – rodzaj pracy)**

**O Ś W I A D C Z E N I E**

**o zapoznaniu się z Polityką Bezpieczeństwa Informacji  
w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu   
oraz o zobowiązaniu się do zachowania poufności**

Oświadczam, że zapoznałam/-em się z Polityką Bezpieczeństwa Informacji Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu i zobowiązuję się do przestrzegania zawartych w niej zasad, reguł i postanowień. Ponadto zobowiązuję się do:

* zachowania w tajemnicy i nie rozpowszechniania bez zgody Pracodawcy, wszelkich informacji nieujawnionych do widomości publicznej, uzyskanych lub wytworzonych w związku z wykonywaniem obowiązków służbowych;
* zachowania w tajemnicy powyższych informacji zarówno w czasie trwania umowy o pracę, jak i po jej rozwiązaniu lub wygaśnięciu;
* nierozpowszechniania informacji, których rozpowszechnienie mogłoby naruszyć imię lub interes Pracodawcy.

Jednocześnie przyjmuję do wiadomości, że naruszenie powyższych zobowiązań może skutkować odpowiedzialnością cywilną i karną na podstawie obowiązujących przepisów prawa.

…......................................................

**(podpis)**

**Załącznik 2 do PBI**

**Zarządzenie nr 10 /XVI R/2025**

Wrocław, dn., \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

….....................................................................

**(imię i nazwisko)**

….....................................................................

**(jednostka organizacyjna)**

…......................................................................

**(status)**

**O Ś W I A D C Z E N I E**

**Doktoranta Szkoły Doktorskiej o zapoznaniu się   
z Polityką Bezpieczeństwa Informacji w Uniwersytecie Medycznym   
im. Piastów Śląskich we Wrocławiu, o zobowiązaniu do zachowania poufności**

Oświadczam, że zapoznałam/-em się z Polityką Bezpieczeństwa Informacji Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu i zobowiązuję się do przestrzegania zawartych w niej zasad, reguł i postanowień. Ponadto zobowiązuję się do:

* zachowania w tajemnicy i nie rozpowszechniania bez zgody Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, wszelkich informacji nieujawnionych do widomości publicznej, uzyskanych lub wytworzonych w związku z realizacją moich studiów;
* zachowania w tajemnicy powyższych informacji zarówno w czasie trwania studiów, jak i po ich ukończeniu;
* nierozpowszechniania informacji, których rozpowszechnienie mogłoby naruszyć imię lub interes Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu.

Jednocześnie przyjmuję do wiadomości, że naruszenie powyższych zobowiązań może skutkować odpowiedzialnością cywilną i karną na podstawie obowiązujących przepisów prawa.

…......................................................

**(podpis)**

**Załącznik 3 do PBI**

**Zarządzenie nr 10/XVI R/2025**

Wrocław, dn., \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

….....................................................................

**(imię i nazwisko)**

….....................................................................

**(jednostka organizacyjna)**

…......................................................................

**(status – rodzaj pracy, aktywności)**

**O Ś W I A D C Z E N I E**

**o zapoznaniu się z Polityką Bezpieczeństwa Informacji  
w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu   
oraz o zobowiązaniu się do zachowania poufności**

Oświadczam, że zapoznałam/-em się z Polityką Bezpieczeństwa Informacji Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu i zobowiązuję się do przestrzegania zawartych w niej zasad, reguł i postanowień. Ponadto zobowiązuję się do:

* zachowania w tajemnicy i nie rozpowszechniania bez zgody Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, wszelkich informacji nieujawnionych do widomości publicznej, uzyskanych lub wytworzonych w związku z realizacją moich obowiązków;
* zachowania w tajemnicy powyższych informacji zarówno w czasie trwania umowy, jak i po jej rozwiązaniu lub wygaśnięciu
* nierozpowszechniania informacji, których rozpowszechnienie mogłoby naruszyć imię lub interes Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu.

Jednocześnie przyjmuję do wiadomości, że naruszenie powyższych zobowiązań może skutkować odpowiedzialnością cywilną i karną na podstawie obowiązujących przepisów prawa.

…......................................................

**(podpis)**