Załącznik
do Zarządzenia nr 109/XV R/2017
Rektora Uniwersytetu Medycznego we Wrocławiu
z dnia 31 października 2017 r.

UNIWERSYTET MEDYCZNY
IM. PIASTÓW ŚLĄSKICH WE WROCŁAWIU

Z A T W I E R D Z AM

Egz. pojedynczy

_____
Rektor
Uniwersytetu Medycznego
we Wrocławiu

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu

WROCŁAW

2017

Strona kontroli dokumentu

Wersja Nr	Data	Przyczyna zmiany

§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 we Wrocławiu wprowadzając Politykę Bezpieczeństwa Informacji (zwaną dalej PBI) deklaruje, że wdrożony System Zarządzania Bezpieczeństwem Informacji w Uniwersytecie Medycznym (SZBI), który jest częścią całościowego systemu zarządzania, będzie podlegał ciągłemu doskonaleniu, zgodnie z wymaganiami norm PN-ISO/IEC 27001 oraz PN-EN ISO 9001. Jednocześnie deklaruje wsparcie dla realizacji przyjętej PBI, a także zapewnienie odpowiednich środków do jej wdrożenia.

§2

Słownik terminów

Występujące w Polityce Bezpieczeństwa Informacji 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 własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

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

§3

Regulacje ogólne

1. Życie i zdrowie osób 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 we Wrocławiu, a w szczególności:
   - informacje przetwarzane w Uniwersytecie Medycznym, niezależnie od formy ich 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.
4. Bezpieczeństwo informacji Uniwersytetu Medycznego we Wrocławiu obejmuje nie tylko jego siedzibę, ale także wszelkie 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 Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji 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 Systemu Zarządzania Bezpieczeństwem Informacji.

§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 i opiekuńczo - medycznych przez:
   - ograniczenie wpływu szeroko pojętych zagrożeń natury teleinformatycznej (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.
2) 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.

3) 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 zasad 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.

Skuteczna ochrona zasobów informacyjnych Uniwersytetu Medycznego wymaga wspólnego działania i zaangażowania wszystkich pracowników, a także studentów i doktorantów.

Obowiązek ochrony zasobów Uniwersytetu Medycznego, w przypadku współpracy z kontrahentami i jednostkami zewnętrznymi, określany jest w ramach umów zawartych z tymi podmiotami.

Pracownicy Uniwersytetu Medycznego zobowiązani są do używania zasobów informacyjnych Uniwersytetu Medycznego wyłącznie do celów służbowych, chyba że regulacje szczegółowe stanowią inaczej. Wszelkie wykonywane operacje w sieci komputerowej Uczelni (z pocztą elektroniczną włącznie), w szczególności dotyczące zasobów wrażliwych pod względem poufności, mogą być monitorowane.

2. Podstawowe zasady bezpieczeństwa informacji

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

1) Zasada uprawnionego dostępu – każdy pracownik zapoznał się z Polityką Bezpieczeństwa Informacji, 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) mechanizmem. 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 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 – skuteczne zabezpieczenie jest 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;
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;
17) 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 pomieszczeń. Indywidualnego hasła nie należy przekazywać ani przełożonemu, ani administratorom, a jeśli do tego doszło należy je zmienić przy pierwszej okazji;

18) 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;

19) Zasada czystego biurka – należy unikać pozostawiania bez nadzoru dokumentów na biurku. Po godzinach pracy wszystkie dokumenty stanowiące tajemnicę Uniwersytetu Medycznego muszą być przechowywane w zamkniętych szafkach, szufladach, regałach itp.;

20) Zasada czystej tablicy – po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice (flipchart, itp.);

21) 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;

22) 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;

23) 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.);

24) Zasada odpowiedzialności za zasoby - każdy użytkownik odpowiada za udostępnione mu zasoby (komputery, oprogramowanie, systemy, konta, itp.)

§6

Odpowiedzialność za bezpieczeństwo informacji w Uniwersytecie Medycznym

1. Odpowiedzialność za bezpieczeństwo informacji w Uniwersytecie Medycznym ponoszą

wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Władze Uniwersytetu Medycznego są odpowiedzialne za zapewnienie warunków niezbędnych do funkcjonowania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Każdy pracownik Uniwersytetu Medycznego, jak również doktorant, student, stażysta, rezydent, praktykant, wolontariusz itp. ma 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 działań zapobiegających zagrożeniom utraty bezpieczeństwa informacji.

2. Jednostki sprawujące nadzór nad realizacją PBI w Uniwersytecie Medycznym

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

1) Pełnomocnik Rektora ds. Ochrony Informacji Niejawnych odpowiedzialny za całokształt spraw związanych z ochroną informacji niejawnych;
2) Administrator Bezpieczeństwa Informacji odpowiedzialny za całokształt spraw związanych z ochroną danych osobowych;
3) W razie konieczności Rektor powołuje Zespół Bezpieczeństwa Informacji (zwany dalej ZBI), w którego skład, w zależności od potrzeb, mogą wchodzić w szczególności:
   - St. Inspektor ds. Obronnych i Obrony Cywilnej,
   - Osoby zatrudnione na stanowiskach ds. ISO,
   - Pełnomocnik Rektora ds. Ochrony Informacji Niejawnych,
   - Audytor Wewnętrzny,
   - Kierownik Działu Organizacyjno-Prawnego,
   - Kierownik Centrum Informatycznego,
   - Pracownik Archiwum Zakładowego,
   - Gł. Specjalista ds. BHP i PPoż.,
   - Administrator Bezpieczeństwa Informacji,
   - Rzecznik Prasowy,
   - Inne osoby, w tym administratorzy systemów teleinformatycznych, których włączenie do Zespołu okaże się konieczne.

ZBI przygotowuje ocenę funkcjonowania mechanizmów bezpieczeństwa informacji w Uniwersytecie Medycznym i przedstawia propozycje dokonania zmian w stosownych

dokumentach, procedurach, infrastrukturze technicznej itp. Szczegółowy zakres zadań ZBI określa Rektor w zarządzeniu o jego powołaniu.

3. Sankcje za naruszenie zasad bezpieczeństwa informacji

Nieprzestrzeganie zasad zawartych w dokumencie Polityki Bezpieczeństwa Informacji jest naruszeniem obowiązków pracowniczych i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie pracownika do odpowiedzialności wynikającej z przepisów prawa i Regulaminu Pracy.

§7
Wymagania

1. Każdy pracownik jak również doktorant, student, stażysta, rezydent, praktykant, wolontariusz itp. Uniwersytetu Medycznego ma obowiązek zapoznania się z PBI.
2. Każdy pracownik i doktorant Uniwersytetu Medycznego powinien podpisać oświadczenie o zapoznaniu się z dokumentem Polityki Bezpieczeństwa Informacji.
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
Rozpowszechnianie i zarządzanie dokumentem Polityki Bezpieczeństwa Informacji

1. Zaleca się rozpowszechnianie niniejszego dokumentu wśród pracowników Uniwersytetu Medycznego, jego partnerów i klientów, wybranych urzędów lub organów administracji publicznej, jako dowodu zwracania szczególnej uwagi na bezpieczeństwo informacyjne Uniwersytetu Medycznego i jego partnerów.
2. Za zarządzanie niniejszym dokumentem, w tym jego rozpowszechnianie, aktualizację, utrzymywanie spójności z innymi dokumentami odpowiedzialny jest Pełnomocnik ds. Ochrony Informacji Niejawnych.

§9
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 27 lipca 2005 r. - Prawo o szkolnictwie wyższym (Dz.U. z 2016 r., poz.

1842 ze zm.);

- Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2016 r., poz. 1638 ze zm.);
- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2017 r., poz.1845 ze zm.) wraz z mającymi zastosowanie aktami wykonawczymi;
- Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2017 r., poz. 1318 ze zm.);
- Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. z 2017 r., poz. 459 ze zm.);
- Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (Dz.U. z 2016 r., poz. 1137 ze zm.);
- Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz.U. z 2016 r., poz. 1666 ze zm.);
- Ustawa z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz.U. z 2017 r., poz. 1257);
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922);
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r., poz. 1167 ze zm.);
- Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2003 r., Nr 153, poz. 1503 ze zm.);
- Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2016 r., poz. 1432 ze zm.);
- Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2016, poz. 1047 ze zm.);
- Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2017 r., poz. 880 ze zm.);
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2016 r., poz 1764);
- Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. z 2015 r., poz. 1341);
- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001 r. Nr 128, poz.1402, z późn. zm.).
- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r. poz.1579, z późn. zm.).

ZAŁĄCZNIKI:

Załącznik – Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Uniwersytecie Medycznym im. Piastów Śląskich we Wrocławiu.

OPRACOWAŁ

Pełnomocnik ds. Ochrony
Informacji Niejawnych
Uniwersytetu Medycznego
we Wrocławiu

Wykonano w egz. pojedynczym
W.B. (tel. +48717841541)