1. Cel i zakres opracowania Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji (PBI) wyraża wolę *Najwyższego kierownictwa* UCK w zakresie spełnienia mających zastosowanie wymagań dotyczących *Bezpieczeństwa informacji* oraz ochrony jego *Zasobów informacyjnych*, a także wyznacza główne kierunki działania *Kierownictwa* oraz *Pracowników* w celu zapewnienia systemowego nadzoru nad *Przetwarzaniem informacji*, w tym m.in. ich zbieraniem, opracowywaniem, przechowywaniem i udostępnianiem, niezależnie od sposobu realizacji tych *Procesów*.

Celem Polityki Bezpieczeństwa Informacji jest przedstawienie obowiązujących w UCK podstawowych zasad ustanowionych w celu spełnienia ww. wymagań oraz zapewnienia bezpieczeństwa przetwarzanych przez UCK *Informacji*, w tym zapewnienia ich *Poufności*, *Integralności*, *Dostępności* i *Autentyczności*.

PBI określa strukturę zarządzania *Bezpieczeństwem Informacji* oraz definiuje ogólne pojęcia, a także wymagania i zasady kluczowe dla zapewnienia *Poufności*, *Integralności*, *Dostępności* i *Autentyczności*, a – w przypadku wykorzystywania *Systemów informacyjnych* – także *Autentyczności* przetwarzanych przez UCK *Informacji*, zgodnie z którymi są zarządzane, zabezpieczane i eksploatowane *Aktywa informacyjne* UCK.

2. Terminy i definicje

Ilekroć w dokumencie jest mowa o terminach związanych z funkcjonowaniem *Systemu Zarządzania Bezpieczeństwem Informacji* (*SZBI*), należy przez to rozumieć terminy w znaczeniu wskazanym w **„Leksykonie Uniwersyteckiego Centrum Klinicznego"**, a zwłaszcza w znaczeniu wskazanym w części zatytułowanej „System Zarządzana Bezpieczeństwem Informacji (SZBI)". Leksykon stanowi **załącznik nr 10 do Księgi Zintegrowanego Systemu Zarządzania.**

3. Deklaracja Najwyższego Kierownictwa

Dyrektor Naczelny - stojąc na stanowisku, że *Informacja* jest kluczowym *Zasobem* UCK i wpływa na ciągły jego rozwój oraz możliwość właściwej realizacji usług świadczonych przez UCK - wyraża wolę w zakresie spełnienia mających zastosowanie wymagań dotyczących *Bezpieczeństwa informacji* oraz ochrony *Zasobów informacyjnych* UCK, w tym zwłaszcza przetwarzanych *Danych osobowych*, której przejawem jest **„Deklaracja Polityki Bezpieczeństwa Informacji"**, stanowiąca rozdział Księgi Zintegrowanego Systemu Zarządzania, zgodnie z uwarunkowaniami prawnymi określonymi w niniejszym dokumencie.

Dyrektor Naczelny zobowiązuje się do *Ciągłego doskonalenia SZBI* oraz deklaruje podjęcie działań niezbędnych do zapewnienia pełnego zintegrowania wdrożonego *SZBI* z *Systemem Zarządzania Ciągłością Działania* i *Zintegrowanym Systemem Zarządzania* oraz zapewnienia jego zgodności z celami funkcjonowania UCK, w tym ze strategią rozwoju UCK, w tym długofalową **„Strategią Uniwersyteckiego Centrum Klinicznego na lata 2022-2025 r."**, a także celami i planami strategicznymi na dany rok.

4. Uwarunkowania prawne

Polityka Bezpieczeństwa Informacji (PBI) jest zgodna z prawem Rzeczpospolitej Polskiej oraz prawem Unii Europejskiej, a także opiera się na polskich normach i standardach międzynarodowych, a w szczególności na normie PN-EN ISO/IEC 27001.

Wykaz aktów normatywnych, polskich norm oraz standardów międzynarodowych, na podstawie których opierają się postanowienia niniejszej Polityki Bezpieczeństwa Informacji, stanowi **załącznik nr 11 do Księgi Zintegrowanego Systemu Zarządzania - „Wykaz dokumentów związanych z Polityką Bezpieczeństwa Informacji".**

5. Zakres Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

System Zarządzanie Bezpieczeństwem Informacji (*SZBI*) (w tym poszczególne *Procesy* i interakcje między nimi) został ustanowiony, wdrożony oraz jest utrzymywany i ciągle doskonalony w oparciu o normę PN-EN ISO/IEC 27001.

W celu określenia granic i możliwości zastosowania *SZBI*, a w konsekwencji ustanowienia jego zakresu, uwzględniono:

- *Kontekst wewnętrzny* oraz *Kontekst zewnętrzny*, w jakim funkcjonuje UCK, w tym czynniki wewnętrzne i zewnętrzne, które są istotne dla celu jego działania oraz takie, które wpływają na zdolność UCK do osiągnięcia zamierzonych wyników działania ww. *SZBI*,
- istotne dla *SZBI Strony zainteresowane* oraz ich wymagania, obejmujące w szczególności uwzględnione w ramach *SZBI* wymagania wynikające z przepisów prawa powszechnie obowiązującego, wymagania regulacyjne oraz zobowiązania umowne,
- zależności między działaniami realizowanymi przez UCK oraz *Podmioty zewnętrzne*.

Zakres *SZBI* jest właściwy dla prowadzonej przez UCK działalności, tj. dotyczy *Procesów* związanych z udzielaniem świadczeń zdrowotnych, w tym m.in. w zakresie diagnostyki, leczenia stacjonarnego, ambulatoryjnego oraz rehabilitacji (ze szczególnym uwzględnieniem świadczeń wysokospecjalistycznych w ramach poszczególnych specjalności), a także obrotu i dystrybucji produktów leczniczych przez Aptekę Szpitalną. *SZBI* odnosi się do całej organizacji i wszystkich realizowanych w niej *Procesów*. Oznacza to, że ochrona *Informacji* zgodnie z wdrożonym *SZBI*, obejmuje:

- wszystkich *Pracowników* (bez względu na status *Użytkowników Systemów informacyjnych* UCK), a także inne osoby i podmioty uzyskujące dostęp do *Zasobów informacyjnych* UCK na podstawie przyjętego na siebie - na podstawie umów, porozumień lub innych stosunków prawnych - zobowiązania dotyczącego przestrzegania jej zasad, w tym *Stałych współpracowników* i inne *Podmioty zewnętrzne,*
- wszystkie pomieszczenia, w których przetwarzane są *Informacje* podlegające ochronie w UCK,
- *Informacje* przetwarzane w UCK, niezależnie od ich formy i *Nośnika informacji*, na jakim zostały utrwalone,
- *Urządzenia końcowe* i inne urządzenia wykorzystywane przez UCK do *Przetwarzania informacji,* a także inne *Nośniki informacji* (np. elektroniczne i optyczne), na których znajdują się *Informacje* podlegające ochronie,
- technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu *Informacji*, w tym m.in. *Systemy informacyjne* oraz wykorzystywane przez UCK oprogramowanie.

6. Ogólne zasady ochrony zasobów informacyjnych

Aktywa informacyjne UCK są chronione z należytą starannością i w sposób adekwatny do ich wrażliwości i krytyczności.

Pracownik, przed uzyskaniem dostępu do *Zasobów informacyjnych* UCK, zapoznawany jest z zasadami dotyczącymi *Bezpieczeństwa informacji* oraz aktualnymi procedurami ochrony *Informacji* w UCK, w tym również odnoszącymi się do danego stanowiska pracy. Ewentualne dodatkowe postanowienia dotyczące ochrony *Informacji* i zachowania ich w *Poufności*, w tym terminów jej zachowania oraz wiążącej się z tym odpowiedzialności, określane są – w zależności od potrzeb – w zawieranych z *Pracownikami* umowach.

Obowiązek ochrony *Zasobów informacyjnych* UCK, w tym przestrzegania postanowień niniejszej Polityki, przez inne niż *Pracownicy* osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej, a zwłaszcza współpracujące z UCK *Podmioty zewnętrzne*, określany jest w ramach zawieranych z nimi umów.

W ramach ustanowionego i wdrożonego *SZBI* UCK objęło nadzorem wszystkie funkcjonujące i podejmowane przez siebie *Procesy*. Podejście procesowe odzwierciedla zastosowany przez UCK cykl Deminga (cykl PDCA). Oparty o cykl PDCA *SZBI* pozwala na całościowe i skoordynowane spojrzenie na *Ryzyko* odnoszące się do *Bezpieczeństwa informacji* oraz wdrożenie kompleksowego zestawu *Zabezpieczeń* ww. *Informacji*. Szczegółowe *Informacje* na temat podejmowanych w ramach cyklu PDCA działań zawiera **załącznik nr 1 do niniejszej Polityki – „Fazy postępowania. Cykl Deminga"**.

Podstawą realizacji niniejszej Polityki Bezpieczeństwa Informacji są nw. ogólne zasady:

- ***Zasada uprawnionego dostępu***,
- ***Zasada wiedzy koniecznej*** (***Zasada wiedzy uzasadnionej***),
- ***Zasada świadomości zbiorowej***,
- ***Zasada indywidualnej odpowiedzialności*** (***Zasada rozliczalności***),
- ***Zasada separacji obowiązków***,
- ***Zasada stałej gotowości***,
- ***Zasada kompleksowości***,
- ***Zasada adekwatności***,
- ***Zasada świadomej konwersacji***.

7. Cele Systemu Zarządzania Bezpieczeństwem Informacji

Cele *SZBI* (tzw. cele *Bezpieczeństwa informacji*):

- zagwarantowanie odpowiedniego poziomu *Bezpieczeństwa informacji*,
- zapewnienie – adekwatnego do celów prowadzonej przez UCK działalności oraz wymagań prawa powszechnie obowiązującego – poziomu *Poufności*, *Dostępności*, *Integralności i Autentyczności* przetwarzanych przez UCK *Informacji*, w tym danych powierzonych przez pacjentów oraz inne osoby, a także zapewnienie ciągłości ich przetwarzania,
- zapewnienie zgodności z przepisami prawa powszechnie obowiązującego, wymaganiami kontraktowymi i innymi wymaganiami obowiązującymi w UCK, a odnoszącymi się do organizacji *Bezpieczeństwa informacji*,
- przyczynienie się do poprawnego i bezpiecznego funkcjonowania wszystkich systemów *Przetwarzania informacji*, w tym zapewnienie, że eksploatowane przez UCK *Systemy informacyjne* gwarantują

Niezaprzeczalność nadania, *Niezaprzeczalność odbioru* oraz *Rozliczalność* zadań, a stosowane *Zabezpieczenia* zapewniają odpowiedni poziom *Cyberbezpieczeństwa*,

- wykrywanie *Podatności* wykorzystywanych *Zasobów* oraz maksymalnie ograniczenie możliwości ich wykorzystania przez *Zagrożenia* dla *Bezpieczeństwa informacji*, które wynikają z celowej lub przypadkowej działalności człowieka oraz ich ewentualnych skutków,
- *Zarządzanie cyberbezpieczeństwem* w taki sposób, żeby ograniczyć liczbę występujących *Incydentów cyberbezpieczeństwa* oraz zapewnić odpowiednią reakcję na *Incydenty poważne cyberbezpieczeństwa* oraz *Incydenty krytyczne cyberbezpieczeństwa*, która pozwoli na ograniczenie ich skutków oraz prawdopodobieństwa ich ponownego wystąpienia,
- zapewnienie *Zasobów* niezbędnych do podjęcia działań w sytuacjach zakłócających normalne funkcjonowanie UCK (związanych z zapewnieniem *Ciągłości działania* UCK),
- przyczynienie się do ochrony interesów UCK, w tym utrzymania jego dobrego wizerunku, jako organizacji dbającej o *Bezpieczeństwo informacji*, a tym samym wpłynięcie na ciągłość i efektywność działalności UCK.

Powyższe cele realizowane są poprzez:

- przypisanie odpowiedzialności zgodnie ze strukturą organizacyjną UCK, zapewniające optymalny podział, koordynację zadań i odpowiedzialności związanych z zapewnieniem *Bezpieczeństwa informacji*,
- wyznaczenie *Właścicieli Zasobów* (*Właścicieli Aktywów*) dla *Aktywów* przetwarzających kluczowe *Informacje*, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu *Bezpieczeństwa informacji*,
- przyjęcie do stosowania przez wszystkie osoby i podmioty, które uzyskują dostęp do *Zasobów informacyjnych* UCK, we właściwym zakresie, obowiązujących w UCK polityk i procedur związanych z *Bezpieczeństwem informacji*,
- adekwatne do wykonywanych czynności przeszkolenie osób, które uzyskują dostęp do *Zasobów informacyjnych* UCK,
- *Klasyfikację informacji* i przyporządkowanie im, odpowiednich do wymaganego poziomu ochrony, zasad przetwarzania,
- określenie zasad *Przetwarzania informacji*, w tym mechanizmów gwarantujących ich ochronę oraz wyznaczenie stref, w których może się ono odbywać, a także odpowiednie ich zabezpieczenie,
- *Zarządzanie ryzykiem*, na które składa się:
    - *Identyfikacja ryzyka*,
    - *Estymacja ryzyka*,
    - *Ocena ryzyka*,
    - określenie *Planu Postępowania z Ryzykiem*,
    - *Postępowanie z ryzykiem* (wdrożenie ustalonych w planie środków modyfikujących *Ryzyko*),
    - akceptacja *Ryzyk szczątkowych*,

  (działania odnoszące się zarówno do *Ryzyk*, jak i szans),

- *Zarządzanie zmianami*, na które składa się:
  - analiza wpływu zmian na poziom *Bezpieczeństwa informacji*,
  - zapewnienie pełnej koordynacji *Procesu* wprowadzania zmian,
- *Zarządzanie ciągłością działania* poprzez określenie i wdrożenie instrukcji i procedur awaryjnych, a także zapewnienie, by plany zachowania *Ciągłości działania* były tworzone, utrzymywane i testowane w stopniu umożliwiającym nieprzerwaną realizację zadań statutowych UCK,
- *Zarządzanie incydentami* naruszającymi *Bezpieczeństwo informacji* oraz słabościami *SZBI*, w tym zapewnienie, że wszelkie naruszenia *Bezpieczeństwa informacji* (*Incydenty*) oraz jego słabe punkty są raportowane i badane,
- przegląd i aktualizacja polityk i procedur postępowania dokonywane przez odpowiedzialne osoby (w celu zapewnienia jak najlepszej reakcji na *Zagrożenia* i *Incydenty*),
- prowadzenie działań zmierzających do poprawy poziomu *Bezpieczeństwa informacji*, w tym ciągłe doskonalenie *SZBI* zgodnie z wymaganiami normy PN-EN ISO/IEC 27001 i zaleceniami *Zainteresowanych stron*.

Szczegółowe cele *Bezpieczeństwa informacji* określają poszczególni *Właściciele zasobów.* Cele te winny:

- zostać zakomunikowane oraz być dostępne jako zakomunikowane *Informacje*; należy przy tym określić co ma być zrobione i do kiedy, jakie zasoby będą wymagane, kto będzie odpowiedzialny, a także jak będą oceniane wyniki,
- być spójne z niniejszą PBI,
- być mierzalne (o ile to wykonalne),
- uwzględniać mające zastosowanie wymagania *Bezpieczeństwa informacji*, wyniki *Szacowania ryzyka* i *Postępowania z ryzykiem*,
- być monitorowane,
- być aktualizowane, jeśli to właściwe.

Podkreśla się przy tym, iż w ramach doskonalenia *SZBI* deklarowana jest wola współpracy w zakresie poprawy stanu ochrony *Aktywów informacyjnych* UCK z:

- *Podmiotami zewnętrznymi* potwierdzającymi kompetencje UCK na zgodność ze standardami *Bezpieczeństwa informacji*, w tym na zgodność z normą PN-EN ISO/IEC 27001,
- ekspertami w zakresie *Bezpieczeństwa informacji*, w tym – w szczególności – *CSIRT NASK* oraz innymi podmiotami wchodzącymi w skład *Krajowego systemu cyberbezpieczeństwa,*
- przedstawicielami organów publicznych, w tym – w szczególności – z Prezesem Urzędu Ochrony Danych Osobowych, a także Ministrem właściwym ds. Cyfryzacji oraz organami właściwymi ds. *Cyberbezpieczeństwa*,
- pozostałymi *Podmiotami zewnętrznymi* (m.in. *Klientami* indywidualnymi i instytucjonalnymi, dostawcami, partnerami branżowymi i innymi *Zainteresowanymi stronami*).

8. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji

Dokumentacja *SZBI*, której fundament stanowi niniejsza Polityka Bezpieczeństwa Informacji, została opracowana w celu:

- udokumentowania zasad ochrony *Informacji,* w tym zapewnienia *Cyberbezpieczeństwa* wykorzystywanym do ich przetwarzania *Systemom informacyjnym* na potrzeby skutecznego wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia *SZBI*, w tym wszelkich działań związanych z ochroną *Informacji*,
- zapewnienia poziomu *Bezpieczeństwa informacji*, który spełnia wymagania określone w przepisach prawa powszechnie obowiązującego oraz adresuje *Ryzyka* zidentyfikowane przez *Szacowanie ryzyka*,
- dokładnego informowania *Pracowników*, *Klientów* i innych osób uzyskujących dostęp do *Zasobów informacyjnych* UCK, a także innych *Stron zainteresowanych* świadczonymi usługami o zasadach działania *SZBI* oraz wpływu ich działań na spełnienie wymagań obowiązujących przepisów prawa, a szczególnie zapobiegania popełnianych błędów w tym zakresie,
- uzyskania efektu tzw. „organizacji samouczącej się", dążącej do uzyskania optymalnej jakości świadczonych usług poprzez *Ciągłe doskonalenie* skuteczności działania,
- przekazania *Podmiotom zewnętrznym* współpracującym z UCK na podstawie umów, porozumień lub innych stosunków prawnych obowiązujących w UCK zasad ochrony *Informacji*,
- zachowania należytej dbałości o *Poufność*, *Integralność*, *Dostępność* i *Autentyczność Informacji* podczas kontaktów z pacjentami, *Klientami* i innymi współpracującymi z UCK *Podmiotami zewnętrznymi*.

Dokumentacja *SZBI* składa się z niżej wymienionych elementów, którymi są:

- **KJ-DZ 3.2 – „Deklaracja Polityki Bezpieczeństwa Informacji"**,
- **KJ-DZ 21.0 - „Polityka Bezpieczeństwa Informacji" (PBI)**,
- **KJ-DZ 22.0 - „Polityka zarządzania ryzykiem"**,
- **KJ-DZ 23.0 – „Polityka zarządzania ciągłością działania"**,
- **KJ-DZ 24.0 – „Polityka zarządzania zabezpieczeniami kryptograficznymi"**,
- **KJ-DZ 26.0 – „Polityka usług chmurowych"**,
- procedury i instrukcje bezpieczeństwa, które określają szczegółowe zasady postępowania, wymienione w **załączniku nr 11 do Księgi Zintegrowanego Systemu Zarządzania – „Wykaz dokumentów związanych z Polityką Bezpieczeństwa Informacji"**,
- **„Deklaracja Stosowania"**,
- dokumentacja operacyjna z zakresu nadzoru nad *SZBI*.

Przepisy prawa powszechnie obowiązującego mają moc nadrzędną nad zapisami wdrożonego w UCK *SZBI*, w tym zapisami niniejszej Polityki Bezpieczeństwa Informacji oraz wynikającej z niej dokumentacji podrzędnej.

Polityka Bezpieczeństwa Informacji (PBI) jest dokumentem nadrzędnym nad inną dokumentacją dotyczącą *Bezpieczeństwa informacji*, wchodzącą w zakres *SZBI*. Dokumentacja związana z *Bezpieczeństwem informacji* jest podporządkowana niniejszej Polityce. Zasady określone w dokumentacji *SZBI* należącej do kolejnych poziomów nie mogą pozostawać w sprzeczności z treścią dokumentacji z poziomów nadrzędnych.

Rozwiązywanie ewentualnej kolizji treści dokumentacji wchodzącej zakres *SZBI* leży w kompetencjach Pełnomocnika DN ds. SZBI.

Rozwiązywanie ewentualnej kolizji PBI z pozostałą dokumentacją *ZSZ* leży w kompetencjach właściwej merytorycznie *Komórki organizacyjnej* UCK / *Właściciela Zasobu* przy współpracy z Pełnomocnikiem DN ds. SZBI oraz Pełnomocnikiem DN ds. SZ.

9. Struktura zarządzania bezpieczeństwem informacji i podział odpowiedzialności

9.1. Poziomy działań

UCK określiło i zapewniło zasoby potrzebne do ustanowienia, wdrożenia, utrzymywania i *Ciągłego doskonalenia SZBI.*

Przy podziale ról w strukturze organizacyjnej, UCK kieruje się następującymi zasadami:

- oddzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych,
- uniemożliwienie nadużyć i maksymalne ograniczenie błędów popełnianych przez pojedyncze osoby,
- zakomunikowanie odpowiedzialności i uprawnień.

W strukturze zarządzania *Bezpieczeństwem informacji* wyróżnia się trzy poziomy działań, tj.:

- **na poziomie strategicznym** – prowadzona jest ogólna polityka *Bezpieczeństwa informacji* w odniesieniu do wcześniej rozpoznanego, określonego, a także poddanego *Analizie ryzyka* i zasadniczych oczekiwań co do poziomu *Bezpieczeństwa informacji* oraz w odniesieniu do wynikających z nich modelowych zadań i rozwiązań (w te *Procesy* zaangażowane jest *Najwyższe Kierownictwo* UCK określające zasadnicze kryteria *Bezpieczeństwa informacji* – pochodne od kryteriów normatywnych i możliwe do zrealizowania na bazie zidentyfikowanych atrybutów *Informacji*), a także zatwierdzane są sposoby *Postępowania z ryzykiem* oraz zapewniane *Zasoby* niezbędne do ustanowienia odpowiednich *Zabezpieczeń,*
- **na poziomie taktycznym** – tworzone są standardy *Bezpieczeństwa informacji* oraz zasady kontroli ich wypełniania w stosowanych rozwiązaniach i *Systemach informacyjnych* oraz przestrzegania w praktyce używania ww. rozwiązań i *Systemów informacyjnych* (w te *Procesy* zaangażowani są głównie kierownicy *Komórek organizacyjnych* UCK oraz osoby zajmujące samodzielne stanowiska zgodnie ze schematem organizacyjnym UCK), identyfikowane są szanse oraz *Ryzyka* dla realizacji *Procesów* z zachowaniem zasad i wymagań *Bezpieczeństwa informacji* oraz realizowane działania związane z monitorowaniem skuteczności *SZBI,*
- **na poziomie operacyjnym** – prowadzona jest administracja *Bezpieczeństwem informacji* pod kątem pełnego stosowania standardów bezpieczeństwa oraz rozwiązywania ewentualnych przypadków zakłóceń wynikających z naruszenia tych standardów (intencjonalnego lub przypadkowego), odbywa się raportowanie niezgodności i *Incydentów.*

Rys. 1. Diagram – poziomy działań w strukturze zarządzania *Bezpieczeństwem informacji.*

Skuteczna ochrona *Aktywów informacyjnych* UCK wymaga wspólnego działania i zaangażowania wszystkich *Pracowników* oraz innych osób dopuszczonych do *Aktywów informacyjnych* UCK.

9.2. Odpowiedzialność poszczególnych osób za *Bezpieczeństwo informacji*

Odpowiedzialność za *Bezpieczeństwo Informacji* w UCK ponoszą wszyscy *Pracownicy*, zgodnie z posiadanymi zakresami obowiązków oraz wszystkie inne osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej dopuszczone do *Zasobów Informacyjnych* UCK, zgodnie przyjętymi na siebie zobowiązaniami.

Kierownicy *Komórek organizacyjnych* UCK oraz wyznaczeni do nadzorowania PBI *Pracownicy* realizują obowiązki związane z utrzymaniem *Bezpieczeństwa informacji*, w ramach których podejmują działania związane z:

- nadzorem i kontrolą przestrzegania PBI oraz zapewnieniem zgodności funkcjonującego *SZBI*, odnośnie realizowanych przez nadzorowaną *Komórkę organizacyjną* UCK działań, z wymaganiami przepisów prawa powszechnie obowiązującego oraz innych regulacji, w tym m.in. z wymaganiami normy PN-EN ISO/IEC 27001,
- przedstawiania *Najwyższemu Kierownictwu* wyników działania *SZBI*, odnośnie realizowanych przez nadzorowaną *Komórkę organizacyjną* UCK działań.

Od tych *Pracowników* wymagana jest szczególna lojalność, staranność oraz wysoka etyka zawodowa.

Kierownicy *Komórek organizacyjnych* UCK odpowiedzialni są za ochronę *Bezpieczeństwa informacji* w danej *Komórce organizacyjnej* UCK, a w szczególności za monitorowanie *Poufności, Integralności, Dostępności* i *Autentyczności* w odniesieniu do *Informacji* oraz odpowiednio do rodzaju posiadanych *Zasobów informacyjnych*, nadzorowanie przestrzegania zasad *Bezpieczeństwa informacji* przez podległych *Pracowników* oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia *Incydentu* lub sytuacji mogącej prowadzić do wystąpienia *Incydentu*.

Przełożeni *Pracowników* wszystkich szczebli odpowiadają za nadzór nad realizacją zadań wykonywanych przez podlegających im *Pracowników*, wynikających z Polityki Bezpieczeństwa Informacji.

Wszyscy *Pracownicy* oraz wszystkie inne osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej dopuszczone do *Zasobów Informacyjnych* UCK, w tym współpracujące

z UCK ***Podmioty zewnętrzne*** zobowiązani są do ochrony *Zasobów informacyjnych* UCK i dbałości o ich *Poufność*, *Integralność*, *Dostępność* i *Autentyczność*, w tym do:

- znajomości i przestrzegania zapisów niniejszej Polityki Bezpieczeństwa Informacji (PBI) oraz – o ile ma zastosowanie – pozostałej dokumentacji *SZBI*, tj. w szczególności wdrożonych procedur, instrukcji, zarządzeń, a także do respektowania podjętych przez UCK decyzji mających na celu ochronę jego *Zasobów informacyjnych* oraz wykonywania poleceń osób wyznaczonych do wykonywania zadań związanych z zapewnieniem *Bezpieczeństwa informacji,*
- zachowania w *Poufności* podlegających ochronie *Informacji*, do których uzyskają dostęp w związku z wykonywanymi obowiązkami, zarówno w trakcie trwania stosunku pracy lub innego stosunku prawnego stanowiącego podstawę wykonywania pracy na rzecz UCK, jak i po ich ustaniu,
- dokładania wszelkich starań, aby chronić powierzone im do używania *Zasoby* UCK, a zwłaszcza do stosowania wymaganych *Zabezpieczeń* mających na celu ochronę *Zasobów informacyjnych* UCK przed ich udostępnieniem osobom nieuprawnionym,
- przeciwdziałania próbom naruszenia *Bezpieczeństwa informacji*,
- informowania o wystąpieniu *Incydentu związanego z bezpieczeństwem informacji,* w tym *Incydentu cyberbezpieczeństwa* i innego *Zdarzenia związanego z bezpieczeństwem informacji, w tym* o wszelkich zidentyfikowanych słabościach *SZBI*,
- zaangażowania w doskonalenie *SZBI*, w tym zwłaszcza:
  - zgłaszania propozycji zmian w *Procesie*, procedurze lub innym dokumencie,
  - przekazywania *Informacji* o jakie zwracają się osoby odpowiedzialne za zapewnienie *Bezpieczeństwa teleinformatycznego,* w szczególności Pełnomocnik DN ds. SZBI, Pełnomocnik DN ds. SZ, Dyrektorzy Pionów oraz Kierownik Działu Informatyki, Kierownik Działu Teletechniki i kierownicy innych *Komórek organizacyjnych* UCK,
  - uczestnictwa w przeprowadzanych przez UCK szkoleniach z zakresu *SZBI*.

O *Incydencie* należy niezwłocznie poinformować *Właściciela Zasobu* oraz Pełnomocnika DN ds. SZBI, a w przypadku jego nieobecności niezwłocznie powiadomić Dyrektora Naczelnego lub inną osobę – zgodnie ze schematem postępowania, o którym mowa w **procedurze PZ-ZI-02 – „Zarządzanie incydentami i słabościami Systemu Zarządzania Bezpieczeństwem Informacji".**

O innych zdarzeniach mających wpływ na ochronę *Informacji* (w szczególności stwierdzonych lub podejrzewanych *Zagrożeniach* lub *Podatnościach Zasobów*) należy poinformować *Właściciela Zasobu* (w sposób określony w procedurach *SZBI*, a w przypadku *Klientów* lub *Podmiotów zewnętrznych* zgodnie z postanowieniami zawartych z UCK umów) (postanowienia tych umów winny być zgodne z postanowieniami ww. procedury).

Wszelkie działania w zakresie potrzeby opracowania lub wdrożenia ewentualnych zmian w dokumentacji *SZBI* zgłaszane są do Pełnomocnika DN ds. SZBI, który podejmuje współpracę z Pełnomocnikiem DN ds. SZ lub *Zespołem ds. bezpieczeństwa informacji* w zakresie koordynacji działań w tym zakresie. Działania te są podejmowane w miarę zgłaszanych potrzeb, niezależnie od okresowego przeglądu dokumentacji.

9.3. Właściciel zasobu (Właściciel aktywu)

Właściciel zasobu (*Właściciel aktywu*) odpowiada za bieżące nadzorowanie oraz zarządzanie *Aktywem*, tj. utrzymanie wyznaczonego poziomu bezpieczeństwa powierzonego mu *Aktywu* poprzez regulacje wewnętrzne UCK, w tym za współpracowanie z *Zespołem ds. bezpieczeństwa informacji* w zakresie *Szacowania ryzyka*, utworzenie *Planu postępowania z ryzykiem*, dobór *Zabezpieczeń* oraz *Planu ciągłości działania*, nawet w przypadku, gdy za bieżące utrzymywanie *Aktywu* odpowiada *Podmiot zewnętrzny*.

Właściciel zasobu (*Właściciel aktywu*) odpowiedzialny jest również za:

- udostępnienie Pełnomocnikowi DN ds. SZBI oraz *Zespołowi ds. bezpieczeństwa informacji* wszelkich danych niezbędnych do opracowania, wdrożenia i doskonalenia zmian w *SZBI*,
- informowania o poziomie *Bezpieczeństwa informacji* w zakresie przypisanego mu *Zasobu* (*Aktywu*),
- tworzenie i aktualizację procedur postępowania z udziałem wykonawców zadań,
- nadzór nad przestrzeganiem obowiązujących procedur.

9.4. Administrator zasobu (Administrator aktywu)

Administrator zasobu (*Administrator aktywu*) odpowiada za realizację i nadzór nad technicznymi aspektami *Aktywu* w ścisłej kooperacji z *Właścicielem zasobu* (*Właścicielem aktywu*) oraz Pełnomocnikiem DN ds. SZBI.

Administrator zasobu teleinformatycznego (*Administrator systemu*) jest odpowiedzialny za nadzorowanie bezpiecznej eksploatacji i utrzymania oddanego mu do administrowania *Systemu informacyjnego* UCK oraz wspomaganie ochrony systemowych *Zasobów informacyjnych* UCK, a w szczególności za:

- właściwe stosowanie *Środków bezpieczeństwa* w. ww. systemie oraz w odniesieniu do urządzeń, które w nim funkcjonują oraz przeciwdziałanie próbom naruszenia *Bezpieczeństwa informacji*, w szczególności *Cyberbezpieczeństwa,*
- przyznawanie uprawnionym osobom ściśle określonych praw dostępu do *Informacji* w *Systemie informacyjnym* UCK oraz prowadzenie ewidencji osób, którym przyznano dostęp do ww. *Systemu informacyjnego*, dokonywanie ich przeglądu, zapewnienie aktualności i *Rozliczalności,*
- dokonywanie aktualizacji ww. *Systemu informacyjnego* oraz wsparcie działań związanych z jego rozwojem,
- współpracowanie z dostawcą ww. *Systemu informacyjnego*,
- współpracowanie z Pełnomocnikiem DN ds. SZBI, Pełnomocnikiem DN ds. SZ oraz innymi osobami przy opracowaniu projektów procedur, instrukcji oraz dokumentacji wykonawczej lub zmian w ww. dokumentacji odnoszących się do zarządzania ww. *Systemem informacyjnym,*
- udzielanie pomocy technicznej dla *Użytkowników* ww. *Systemu informacyjnego*,
- sporządzanie dotyczącej ww. *Systemu informacyjnego* dokumentacji operacyjnej wynikającej z dokumentacji normatywnej,
- współpracę z osobami odpowiedzialnymi za *Obsługę incydentów cyberbezpieczeństwa.*

9.5. Pełnomocnik Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji (Pełnomocnik DN ds. SZBI)

Pełnomocnik Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji (Pełnomocnik DN ds. ds. SZBI):

- pełni rolę osoby nadzorującej z upoważnienia *Administratora* przestrzeganie w UCK stosowania *Środków technicznych i organizacyjnych* zapewniających ochronę przetwarzanych *Danych osobowych* w sposób odpowiedni do *Zagrożeń* oraz kategorii *Danych osobowych* objętych ochroną,
- koordynuje opracowanie i wdrożenie zmian oraz doskonalenie *SZBI* oraz związanych z nim polityk, procedur, metodyk *Szacowania ryzyka* i mierników poziomu *Zabezpieczeń* dla *SZBI*, a w szczególności:
    - współpracuje z *Komórkami organizacyjnymi* UCK i *Podmiotami zewnętrznymi* w zakresie funkcjonowania *SZBI*, w tym zapewnienia odpowiedniej *Klasyfikacji informacji*,
    - współpracuje z kompetentnymi w zagadnieniach *Bezpieczeństwa informacji* instytucjami, konsultantami i ekspertami zewnętrznymi, a także z jednostkami certyfikującymi w zakresie *SZBI*,
    - nadzoruje przestrzeganie wymagań Polityki Bezpieczeństwa Informacji oraz pozostałej dokumentacji *SZBI*,
    - koordynuje działania *Zespołu ds. bezpieczeństwa informacji,* w tym w zakresie:
        - rozpoznania znaczących zmian *Zagrożeń* i stopnia narażenia *Informacji* lub *Środków przetwarzania informacji* na te *Zagrożenia*,
        - ustalania rekomendacji dla podejmowanych działań przetwarzania *Informacji* i *Zabezpieczeń Zasobów* UCK, w tym priorytetów dla podejmowanych i planowanych działań wdrożenia odpowiedniego poziomu *Zabezpieczeń SZBI*,
    - nadzoruje wdrażanie *Zabezpieczeń*,
    - przedstawia Dyrektorowi Naczelnemu oraz Dyrektorom Pionów okresowe raporty dotyczące funkcjonowania *SZBI*, a także dotyczące wszelkich potrzeb związanych z jego doskonaleniem (zasoby ludzkie, finansowe i inne niezbędne do wdrożenia i zachowania zaplanowanego poziomu *Bezpieczeństwa informacji*),
    - promuje kształcenie, szkolenia i uświadamianie w zakresie *Bezpieczeństwa informacji*, w tym organizuje i prowadzi szkolenia na temat zasad postępowania zgodnych z Polityką Bezpieczeństwa Informacji,
    - współdziała z *Administratorami systemów*, m.in. w zakresie:
        - opracowywania i modyfikacji procedur bezpieczeństwa i standardów *Zabezpieczeń*,
        - opracowywania projektów rozwoju *Systemów informacyjnych* UCK,
        - zapewnienia zgodności *Zarządzania incydentami* dotyczącymi *Cyberbezpieczeństwa* z wymogami *SZBI*,

- ocenia *Informacje* uzyskane z monitorowania i przeglądu *Incydentów* związanych z *Bezpieczeństwem informacji* oraz zaleca odpowiednie działania w stosunku do zidentyfikowanych *Incydentów* związanych z *Bezpieczeństwem informacji*,
- określa postępowanie w przypadku niezgodności polityk i procedur *SZBI* z obowiązującymi aktami normatywnymi lub dokumentacją techniczną.

9.6. Najwyższe Kierownictwo

Najwyższe Kierownictwo odpowiedzialne jest za zapewnienie *Zasobów* niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia *SZBI,* w tym poszczególnych *Zabezpieczeń*, a w szczególności:

- wydaje zgodę na wdrożenie *Systemów informacyjnych* służących do *Przetwarzania informacji* lub *Zabezpieczeń* rekomendowanych przez *Zespół ds. bezpieczeństwa informacji*,
- decyduje o współpracy w zakresie *Bezpieczeństwa informacji* z *Podmiotami zewnętrznymi*,
- wyraża zgodę na udostępnienie stronom trzecim *Informacji* stanowiących *Tajemnicę* UCK.

9.7. Zespół ds. Bezpieczeństwa Informacji

W skład *Zespołu ds. bezpieczeństwa informacji* wchodzą:

- Przewodniczący – Pełnomocnik Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji (Pełnomocnik DN ds. SZBI),
- członkowie stali:
  - Zastępca Dyrektora Naczelnego ds. Organizacji i Zgodności,
  - Zastępca Dyrektora Naczelnego ds. Administracyjno–Technicznych,
  - Dyrektor ds. Lecznictwa, Lekarz Naczelny,
  - Pełnomocnik Dyrektora Naczelnego ds. Systemu Zarządzania (Pełnomocnik DN ds. SZ),
  - Kierownik Działu Administracyjno-Gospodarczego,
  - Kierownik Działu Aparatury Medycznej,
  - Kierownik Działu Inwestycyjno-Eksploatacyjnego,
  - Kierownik Działu Innowacji, Analityki i Wdrożeń Technologii Medycznych,
  - Kierownik Działu Informatyki,
  - Kierownik Działu Teletechniki,
  - Kierownik Działu Koordynacji Obsługi Pacjenta,
  - Kierownik Sekcji Dokumentacji,
  - Specjalista ds. Cyberbezpieczeństwa,
- inne osoby powoływane doraźnie przez Dyrektora Naczelnego na wniosek Pełnomocnika DN ds. SZBI, które mają kluczowe znaczenie dla osiągnięcia zamierzonego celu lub realizacji zadania na rzecz UCK w zakresie zapewnienia właściwego *Bezpieczeństwa informacji*.

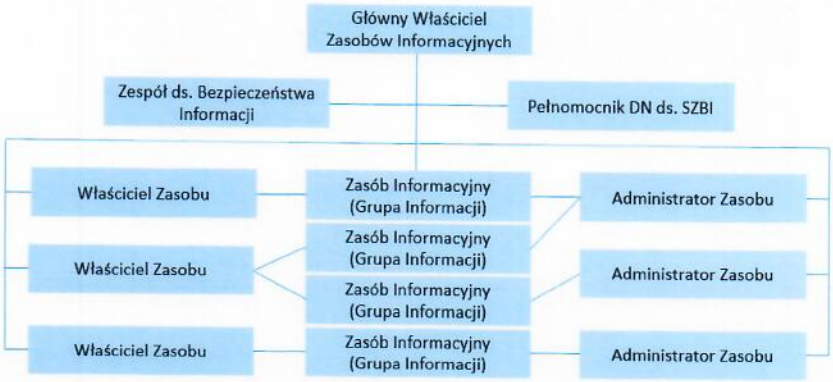
Zespół ds. bezpieczeństwa informacji okresowo, stosownie do potrzeb, zwoływany jest przez Pełnomocnika DN ds. SZBI w porozumieniu z Dyrektorem Naczelnym.

Zespół ds. bezpieczeństwa informacji pełni funkcję doradczą w UCK w zakresie zagadnień związanych z *Bezpieczeństwem informacji*, a przy tym jest odpowiedzialny za inicjowanie oraz wspieranie działań związanych z *Bezpieczeństwem informacji*.

Do zadań *Zespołu ds. bezpieczeństwa informacji* należy:

- dokonywanie okresowego przeglądu Polityki Bezpieczeństwa Informacji oraz pozostałej dokumentacji *SZBI*,
- uzgadnianie ogólnego podziału odpowiedzialności za *Bezpieczeństwo informacji* w odniesieniu do wszystkich obszarów działalności UCK,
- uzgadnianie przedstawionej przez Pełnomocnika DN ds. SZBI metodyki i *Procesów* związanych z *Bezpieczeństwem informacji* (w tym *Szacowanie ryzyka*, *Klasyfikacja informacji*),
- monitorowanie istotnych zmian narażenia *Aktywów informacyjnych* na podstawowe *Zagrożenia*,
- dokonywanie przeglądu *Incydentów*, w tym *Incydentów cyberbezpieczeństwa,* a także analiza danych dotyczących tych *Incydentów* oraz ich monitorowanie,
- analiza, ocena i opiniowanie projektów zmierzających do podniesienia poziomu *Bezpieczeństwa informacji*, w tym zatwierdzanie ważniejszych przedsięwzięć w tym zakresie,
- opiniowanie w zakresie doboru *Zabezpieczeń*,
- koordynacja *Procesów* doskonalenia *SZBI*, w tym wdrażania określonych *Zabezpieczeń* w *Systemach informacyjnych, Procesach* lub usługach,
- zabezpieczanie realizacji Polityki Bezpieczeństwa Informacji w UCK,
- zgłaszanie do Pełnomocnika DN ds. SZBI poprawek i aktualizacji do dokumentacji *SZBI*, w tym do niniejszej Polityki Bezpieczeństwa Informacji,
- wspieranie inicjatyw dotyczących propagowania tematyki *Bezpieczeństwa informacji* w UCK,
- wspieranie Kierownictwa UCK w planowaniu budżetu zapewniającego prawidłowe funkcjonowanie *SZBI* w UCK,
- określanie sposobów przeciwdziałania próbom naruszenia *Bezpieczeństwa informacji*,
- opracowywanie i wsparcie przy wdrażaniu *Planów ciągłości działania* w UCK, a także ich testowanie, ocena i aktualizacja.

Rys. 2. Diagram – uproszczona struktura zarządzania *Bezpieczeństwem informacji* w UCK.



10. Cele stosowania zabezpieczeń i zabezpieczenia

Obowiązujący w UCK *SZBI* został oparty o zdefiniowane w załączniku A do normy PN-EN ISO/IEC 27001 cele stosowania *Zabezpieczeń* i *Zabezpieczenia*, które odnoszą się do poszczególnych obszarów działania UCK, a także w oparciu o wymagania wynikające z obowiązujących przepisów, w tym przepisów o ochronie *Danych osobowych*.

Pracownicy, *Klienci* i *Podmioty zewnętrzne* są zapoznawani ze stosowanymi przez UCK *Zabezpieczeniami* zgodnie z zasadą wiedzy koniecznej – w odniesieniu do *Zasobów*, do których mogą mieć dostęp.

Zabezpieczenia są przez UCK ustanawiane, wdrażane, monitorowane, weryfikowane i – w razie potrzeby – ulepszane w taki sposób, aby:

- zapewniały spełnienie poszczególnych celów związanych z *Bezpieczeństwem informacji* oraz prowadzoną przez UCK działalnością,
- były odpowiednie do ewentualnej szkody, jaką UCK mogłoby ponieść w przypadku braku tych *Zabezpieczeń*,
- stanowiły kompleksową ochronę przetwarzanych *Informacji*,
- zaangażowani w ten *Proces* byli wszyscy niezbędni *Pracownicy*, a także aby odbywało się to przy współpracy z innymi osobami fizycznymi, osobami prawnymi i jednostkami organizacyjnymi nieposiadającymi osobowości prawnej, uzyskującymi dostęp do *Zasobów Informacyjnych* UCK, oraz – o ile to zasadne – przy udziale specjalistycznego doradztwa innych osób / *Podmiotów zewnętrznych*.

Szczegółowe zasady ochrony *Informacji* przetwarzanych w ramach prowadzonej przez UCK działalności, dla każdego z obszarów mających wpływ na *Bezpieczeństwo informacji*, określają – ustanowione na podstawie niniejszej Polityki Bezpieczeństwa Informacji – pozostałe procedury i instrukcje wchodzące w zakres *SZBI*, a także zarządzenia lub podjęte decyzje. *Informacje* o stosowanych *Zabezpieczeniach* zawiera Deklaracja stosowania.

11. Zarządzanie aktywami i ryzykami

UCK zarządza swoimi *Aktywami informacyjnymi* poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. *Aktywa informacyjne* są chronione z należytą starannością i w sposób adekwatny do ich wartości. Odpowiedzialność za nie ponoszą *Właściciele aktywów,* a w zakresie właściwego używania

Pracownicy lub *Podmioty zewnętrzne,* którym UCK powierzyło je do wykorzystywaniu w realizacji określonych zadań na rzecz UCK. Obowiązujące zasady dozwolonego używania *Aktywów* oraz postępowania z *Nośnikami informacji* UCK określiło głównie postanowieniami nw. procedur:

- **PZ-ZI-04 – „Bezpieczeństwo fizyczne i środowiskowe"**,
- **PZ-ZI-05 – „Bezpieczeństwo teleinformatyczne"**,
- **PZ-ZI-06 – „Bezpieczeństwo informacji w zarządzaniu zasobami ludzkimi"**.

Aktywa informacyjne są identyfikowane i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Poszczególnym *Aktywom informacyjnym* przypisuje się ich właścicieli (*Właścicieli aktywów*).

Istotnym elementem zarządzania *Aktywami* i *Ryzykami* w UCK jest przeprowadzanie okresowego *Szacowania ryzyka*. Na podstawie wyników *Analizy ryzyka* opracowywane są *Plany postępowania z ryzykiem* dla *Aktywów* o *Ryzykach* większych niż ustalony poziom *Ryzyka akceptowalnego*. *Ryzyka* są przeglądane w ramach okresowych przeglądów oraz na skutek zaistniałych zmian mających wpływ na *SZBI*.

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru kluczowych działań zawierają **procedury PZ-03 - „Zarządzanie ryzykiem"** oraz **procedury PZ-ZI-01 - „Klasyfikacja informacji"**.

12. Bezpieczeństwo zasobów ludzkich

UCK - celu ograniczenia *Ryzyka* błędu, kradzieży, nadużycia lub niewłaściwego użytkowania *Zasobów* - dba o zapewnienie kompetentnych osób do realizacji wyznaczonych w *Procesach* zadań poprzez:

- określenie niezbędnych kompetencji osób wykonujących pracę mającą wpływ na wyniki dotyczące *Bezpieczeństwa informacji*,
- zapewnienie kompetencji ww. osób dzięki odpowiedniemu ich wykształceniu, szkoleniu lub doświadczeniu,
- o ile ma zastosowanie, podjęcie działań mających na celu uzyskanie niezbędnych kompetencji oraz dokonanie oceny skuteczności tych działań,
- zachowanie udokumentowanych *Informacji* potwierdzających ww. kompetencje.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu m.in. z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania *Pracowników* oraz nawiązywania współpracy, a także ustalonym procedurom dotyczącym modyfikacji i zakończenia zatrudnienia oraz współpracy. Przeprowadzane są również szkolenia oraz uświadamianie dotyczące *Bezpieczeństwa informacji* oraz ochrony *Zasobów* UCK w ramach wdrożonego *SZBI*.

Podejmowane przez UCK działania uświadamiające obejmują m.in.:

- zapoznanie *Pracowników* z treścią niniejszej PBI,
- zakomunikowanie *Pracownikom* ich wkładu w skuteczność *SZBI*, w tym korzyści z doskonalenia wyników dotyczących *Bezpieczeństwa informacji*,
- konsekwencji niezgodności z wymaganiami *SZBI*.

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera procedura **PZ-ZI-06 - „Bezpieczeństwo informacji w zarządzaniu zasobami ludzkimi"**.

13. Bezpieczeństwo fizyczne i środowiskowe

W celu zapewnienia *Bezpieczeństwa informacji* przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami, UCK dba o zapewnienie wysokiego poziomu *Bezpieczeństwa fizycznego* i *Bezpieczeństwa środowiskowego*. W przypadku *Informacji* dotyczących pacjentów oraz *Klientów* UCK istotne jest zapewnienie wszystkich podstawowych aspektów *Bezpieczeństwa informacji – Poufności, Dostępności, Integralności* i *Autentyczności.*

Skuteczna realizacja postawionego celu opiera się na ustanowionym podziale odpowiedzialności i ustanowionych takich praktykach, jak zwłaszcza:

- wyznaczenie *Stref bezpieczeństwa* oraz określenie zasad postępowania w tych strefach,
- wdrożenie fizycznych barier chroniących przed nieautoryzowanym dostępem wszędzie tam, gdzie ma to zastosowanie,
- poprawne administrowanie prawami dostępu do *Aktywów informacyjnych* UCK wraz z wdrożeniem fizycznych barier chroniących przed nieautoryzowanym dostępem,
- wyposażenie w systemy i urządzenia podtrzymujące zasilanie kluczowych *Systemów informacyjnych*,
- wdrożenie działań mających na celu regularne tworzenie i przechowywanie kopii systemów w oddalonych przestrzennie, bezpiecznych lokalizacjach,
- wdrożenie systemów wykrywania i reagowania na próby nieautoryzowanego dostępu i włamań oraz wystąpienia *Zagrożeń* środowiskowych wszędzie tam, gdzie ma to zastosowanie.

W objętych ochroną pomieszczeniach należących do strefy II, osoby nieuprawnione do *Przetwarzania informacji* nie mogą zostać pozostawione bez nadzoru osoby uprawnionej. Dostęp personelu technicznego zajmującego się konserwacją sprzętu, partnerów handlowych, pacjentów oraz innych osób do ww. pomieszczeń, w tym zwłaszcza sekretariatów i innych pomieszczeń administracyjnych, dyżurek lekarskich i pielęgniarskich, gabinetów zabiegowych, a także magazynów i biur, wymaga nadzoru *Pracowników*.

Dostęp do pomieszczeń należących do strefy I mają wyłącznie ściśle określone osoby, w tym osoby uprawnione do tego dostępu w związku z wykonywaniem czynności ściśle związanych z przechowywaniem i zabezpieczeniem przetwarzanych w tych pomieszczeniach *Informacji.*

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera procedura **PZ-ZI-04 - „Bezpieczeństwo fizyczne i środowiskowe"**.

14. Zarządzanie bezpieczeństwem systemów i sieci

W celu zapewnienia *Poufności*, *Integralności*, *Dostępności* i *Autentyczności* przetwarzanych *Informacji*, UCK dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem *Systemów informacyjnych* oraz sieci. Skuteczna realizacja postawionego celu możliwa jest dzięki:

- kompetencjom i świadomości *Pracowników* oraz podpisanym umowom ze specjalistycznymi *Podmiotami zewnętrznymi* administrującymi *Systemami informacyjnymi* i wspomagającymi w tym zakresie UCK,
- opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy,
- nadzorowaniu wprowadzania zmian do infrastruktury technicznej,

- prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach (w celu zapewnienia bezpieczeństwa systemów produkcyjnych),
- nadzorowaniu usług dostarczanych przez strony trzecie, a w szczególności wszelkich wprowadzanych zmian do *Systemów informacyjnych* (dostarczane usługi i wprowadzane zmiany winny być odbierane i akceptowane w sposób świadomy, przy uwzględnieniu ich wpływu na *SZBI*),
- wdrożeniu *Zabezpieczeń* chroniących przed złośliwym lub szkodliwym oprogramowaniem,
- systematycznemu tworzeniu i testowaniu *Kopii bezpieczeństwa*,
- przestrzeganiu opracowanych zasad postępowania z *Nośnikami informacji*,
- bieżącym monitorowaniu *Aktywów informacyjnych* pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu *Systemów informacyjnych*,
- monitorowaniu poziomu *Incydentów* w *Systemach informacyjnych* i wdrożeniu mechanizmów reagowania w sytuacji ich wystąpienia.

Wszystkie *Informacje*, które nie stanowią *Informacji publicznych*, a są przekazywane poza UCK, podlegają zabezpieczeniu. Szczegółowe zasady szyfrowania danych określa **procedura PZ-ZI-05 - „Bezpieczeństwo teleinformatyczne"** oraz **instrukcja IO-AIT-04 - „Instalacja, konfiguracja i korzystanie z VPN"**.

UCK ustanawia i stosuje *Zabezpieczenia* dotyczące *Cyberbezpieczeństwa* o charakterze organizacyjnym i technicznym, które są zgodne z najnowszym stanem wiedzy i zaleceniami zawartymi w normie PN-EN ISO/IEC 27001. Środki bezpieczeństwa są wdrażane odpowiednio i proporcjonalnie do wyników *Szacowania ryzyka dla cyberbezpieczeństwa*, w zakresie niezbędnym do zapewnienia, że *SZBI* w zakresie *Przetwarzania informacji* w *Systemach informacyjnych* osiąga założone wyniki.

Stosowane przez UCK środki bezpieczeństwa zapewniają:

- utrzymanie i bezpieczną eksploatację *Systemu informacyjnego*,
- *Bezpieczeństwo fizyczne* i *Bezpieczeństwo Środowiskowe*, uwzględniające *Kontrolę dostępu*,
- bezpieczeństwo i ciągłość dostaw usług, od których zależy działalność UCK w zakresie *Usług kluczowych*,
- wdrażanie, dokumentowanie i utrzymywanie *PCD* umożliwiających ciągłe i niezakłócone świadczenie *Usług kluczowych* oraz zapewniających *Poufność*, *Integralność*, *Dostępność* i *Autentyczność Informacji*,
- objęcie *Kluczowych systemów informacyjnych* (*KSI*) systemem monitorowania w trybie ciągłym,
- zapobieganie i ograniczanie wpływu *Incydentów cyberbezpieczeństwa* na bezpieczeństwo *KSI*.

Wdrażając środki bezpieczeństwa, które mają na celu zapobieganie i ograniczanie wpływu *Incydentów* na bezpieczeństwo *KSI*, UCK:

- stosuje mechanizmy zapewniające odpowiedni poziom *Cyberbezpieczeństwa*,
- zapewnia odpowiednią aktualizację oprogramowania,
- stosuje ochronę przed nieuprawnioną modyfikacją w *Systemach informacyjnych*,
- zapewnia niezwłoczną reakcję na wykryte *Podatności* lub *Zagrożenia cyberbezpieczeństwa*,
- zapewnia *Zabezpieczenia* przy *Teletransmisji* w przypadku *Informacji* wymienianych z *Podmiotami krajowego systemu cyberbezpieczeństwa*.

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera procedura dla *Użytkowników* – **PZ-ZI-05 - „Bezpieczeństwo teleinformatyczne"** oraz procedura dla

Administratorów systemów i osób odpowiedzialnych za *Bezpieczeństwo teleinformatyczne* – **PZ-ZI-10 - „Organizacja procesów bezpieczeństwa teleinformatycznego w systemach informacyjnych"**.

15. Autoryzacja nowych urządzeń, eksploatacja i utrzymanie zasobów informacyjnych

Każde nowe lub zmienione urządzenie służące do *Przetwarzania informacji* lub inny *Aktyw* mogący w jakikolwiek inny sposób wpływać na *Bezpieczeństwo informacji* powinien ostać zweryfikowany na zgodność z wymaganiami *SZBI* i zaakceptowane przez osobę odpowiedzialną za dany obszar działalności. O ile nie zostało to określone szczegółowo w innych opracowaniach, za dopuszczenie do użytkowania nowych urządzeń oraz innych związanych z *Bezpieczeństwem informacji Aktywów* odpowiada *Właściciel zasobu*.

Konfigurowanie urządzeń oraz instalacja i konfiguracja oprogramowania w *Systemach informacyjnych*, na *Urządzeniach końcowych* i innych urządzeniach jest wykonywana wyłącznie przez upoważnionych do tego *Pracowników* lub *Podmioty zewnętrzne.* Zabronione jest samodzielne instalowanie lub odinstalowywanie jakiegokolwiek oprogramowania.

Zapewnienie *Bezpieczeństwa informacji* w ramach eksploatacji i utrzymania *Systemów informacyjnych* odbywa się w oparciu o przyjęte procedury i instrukcje dla *Administratorów systemów.* W zakresie niezbędnym do prawidłowego korzystania z *Systemów informacyjnych* ich *Użytkownikom* udostępnia się instrukcje lub organizuje szkolenia z zasad bezpiecznego korzystania z *Systemów informacyjnych*.

W celu ochrony przed utratą danych przetwarzanych w *Systemach informacyjnych* regularnie wykonuje się, przechowuje i testuje kopie zapasowe. Kopie zapasowe danych (plików lub konfiguracji *Systemów informacyjnych*) wykonywane są przez *Administratora systemu*.

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera **procedura PZ-ZI-10 - „Organizacja procesów Bezpieczeństwa teleinformatycznego w systemach informacyjnych".**

16. Współpraca z podmiotami zewnętrznymi i osobami trzecimi

16.1. Podmioty zewnętrzne

Każda osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, uzyskująca dostęp do *Zasobów informacyjnych* UCK na podstawie umów, porozumień lub innych stosunków prawnych, zobligowana jest, przed uzyskaniem do nich dostępu, do:

- podpisania wymaganej dokumentacji odnoszącej się do zachowania *Poufności*, w tym do zachowania w *Poufności Informacji* prawnie chronionych,
- podpisania zobowiązania do przestrzegania przepisów prawa powszechnie obowiązującego odnoszących się do *Bezpieczeństwa informacji,* bezpieczeństwa i higieny pracy oraz bezpieczeństwa przeciwpożarowego, a także postanowień niniejszej Polityki oraz uzupełniającej jej dokumentacji i innych wymagań *Bezpieczeństwa informacji* (jeśli mają zastosowanie),
- podpisania odpowiedzialności za ewentualne naruszenie obowiązków dotyczących *Bezpieczeństwa informacji* oraz za ewentualnie wyrządzoną szkodę.

Podkreśla się, iż zawierane przez UCK umowy z *Podmiotami zewnętrznymi* / osobami trzecimi, obok deklaracji o zachowaniu *Poufności,* w tym zachowaniu w *Poufności Informacji* prawnie chronionych oraz zobowiązania do działania zgodnie z przepisami prawa powszechnie obowiązującego, winny określać – o ile mają

zastosowanie - obowiązujące ww. *Podmioty zewnętrzne* / osoby dodatkowe szczegółowe zasady odnoszące się do *Bezpieczeństwa informacji*.

W zakresie relacji z *Podmiotami zewnętrznymi,* które korzystają lub dostarczają towary lub usługi związane z dostępem do *KSI*, UCK zapewnia *Cyberbezpieczeństwo* przez ustalenie:

- zasad dostępu sieci UCK lub poszczególnych *Zasobów* w tych sieciach i wymaganych od *Użytkowników Środków bezpieczeństwa* związanego z *Cyberbezpieczeństwem KSI*,
- zasad kwalifikacji *Podmiotów zewnętrznych* jako *Podmiotów świadczących usługi w zakresie cyberbezpieczeństwa*,
- weryfikacji przestrzegania przez *Użytkowników* wymogów bezpieczeństwa *Informacji* w *KSI*.

Wykaz obowiązujących *Podmioty zewnętrzne* / osoby trzecie kluczowych zasad z zakresu *Bezpieczeństwa informacji*, odnoszący się do *Informacji*, z którymi winny być zgodne wszelkie ewentualne dodatkowe postanowienia umowne, zawiera **ogólnodostępny „Informator bezpieczeństwa informacji" - załącznik nr 2 do niniejszej Polityki**, który został również umieszczony na stronie internetowej UCK (www.uck.pl).

16.2. Klienci i inne osoby

UCK informuje *Klientów* i inne osoby, które mogą przekazywać lub mieć dostęp do *Informacji* lub *Zasobów* UCK o zasadach dotyczących bezpieczeństwa, jakie ich obowiązują, przez publikację tych *Informacji* na stronie internetowej UCK, w zakładce „Bezpieczeństwo informacji".

17. Zasady współpracy z Policją, jednostkami Straży Pożarnej i Straży Miejskiej

Współpraca, w tym wymiana *Informacji* o *Zagrożeniach* w zakresie bezpieczeństwa osób i mienia oraz zakłócania spokoju i porządku publicznego następuje poprzez:

- udzielanie wzajemnej pomocy w realizacji zadań ochrony i zapobieganiu przestępczości,
- udzielanie wyczerpujących informacji o *Zagrożeniach* dla bezpieczeństwa i porządku publicznego,
- współdziałanie w zabezpieczeniu powstałych awarii na obiekcie,
- współdziałanie przy zabezpieczeniu miejsc popełnienia przestępstw i wykroczeń w granicach chronionych obiektów.

Współdziałanie przy zabezpieczeniu miejsc popełnienia przestępstw i wykroczeń w granicach chronionych obiektów realizowane jest poprzez:

- zabezpieczenie śladów na miejscu zdarzenia,
- pomoc w ustaleniu świadków zdarzenia,
- niedopuszczenie osób postronnych na miejsce przestępstwa lub wykroczenia.
- wykonywanie innych zleconych przez Policję czynności.

O zaistniałym pożarze lub awarii *Pracownik* lub inna osoba / inny *Podmiot zewnętrzny* zawiadamia Straż Pożarną oraz Dyrektora Naczelnego. Przybyłe jednostki ratownicze należy niezwłocznie skierować na miejsce *Zdarzenia*.

Szczegółowe postanowienia na temat podejmowanych w tym zakresie działań zostały omówione w dotyczącej tego obszaru dokumentacji *ZSZ*, w tym dokumentacji dotyczącej zdarzeń masowych mogących wystąpić na terenie UCK oraz **Instrukcjach Bezpieczeństwa Pożarowego** każdego budynku.

Współpraca dotycząca *Zarządzania kryzysowego* odbywa się zgodnie z postanowieniami **procedury PZ-08 – „Zarządzanie ciągłością działania UCK".**

18. Udostępnienie informacji

Przed udostępnieniem *Informacji* należy upewnić się, że można ją udostępnić. W przypadku wątpliwości o jej udostępnieniu decyduje *Właściciel zasobu*.

Podstawą do ustalenia zasad udostępniania *Informacji* jest przyjęta przez UCK *Klasyfikacja informacji*. Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera **procedura PZ-06 - „Organizacja i działania zakładowej składnicy akt"** oraz **procedura PZ-11 - „Zasady udostępniania dokumentacji medycznej UCK dla celów naukowych i dydaktycznych oraz przeprowadzania na terenie UCK anonimowych badań ankietowych, testowych i podobnych wśród pracowników oraz pacjentów i ich rodzin"**.

19. Kontrola dostępu

W celu zapewnienia, że dostęp do *Informacji* lub służących do *Przetwarzania informacji* / związanych z *Przetwarzaniem informacji* miejsc, urządzeń lub *Systemów informacyjnych* mają tylko uprawnione osoby, UCK zarządza *Kontrolą dostępu*.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom, które dotyczą m.in.:

- określenia zasad udzielania, zmian i odbioru uprawnień *Użytkowników*,
- zapewnienia, że dostęp do *Systemów teleinformatycznych* możliwy jest wyłącznie dla zarejestrowanych *Użytkowników* po podaniu *Identyfikatora* i *Hasła* (*Identyfikator* winien być unikalny dla każdego *Użytkownika* systemu),
- okresowych przeglądów nadanych uprawnień,
- podziału odpowiedzialności wraz z nadzorowaniem ruchu osobowego na terenie UCK,
- działań mających zapewnić bezpieczeństwo zainstalowanego i wykorzystywanego oprogramowania.

Użytkownicy dysponują indywidualnymi *Kontami użytkowników* umożliwiającymi ich jednoznaczną identyfikację, za pośrednictwem których mogą korzystać z udostępnianych *Zasobów* i usług. Mechanizmy *Uwierzytelniania*, rejestrowania i monitorowania zdarzeń gwarantują *Rozliczalność Użytkowników*.

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawierają **procedura PZ-ZI-05 - „Bezpieczeństwo teleinformatyczne"**, **procedura PZ-ZI-10 - „Organizacja procesów zarządzania bezpieczeństwem informacji w systemach informacyjnych"** oraz **procedura PZ-ZI-04 - „Bezpieczeństwo fizyczne i środowiskowe"**, a także – jeśli dotyczy – powiązane z nimi szczegółowe instrukcje opisujące tryb nadawania, modyfikacji oraz odbioru tych uprawnień.

20. Planowanie zmian. Pozyskanie, rozwój i utrzymanie zasobów informacyjnych

W przypadku, w którym UCK określi potrzebę wprowadzenia zmian w ustanowionym i wdrożonym *SZBI*, zmiany te należy wprowadzić w zaplanowany sposób.

Wszystkie *Procesy* związane z pozyskaniem, rozwojem lub utrzymaniem *Systemów informacyjnych*, w tym wykorzystywanych programów i *Aplikacji*, prowadzone są w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu *Bezpieczeństwa informacji*.

Nadzór nad ww. *Procesami* obejmuje, w szczególności:

- organizację prac rozwojowych zgodnie z przyjętymi w UCK etapami planowania, projektowania, tworzenia i wdrażania,
- uwzględnianie wymogów *Bezpieczeństwa informacji* podczas zakupu lub produkcji/opracowywania nowych *Systemów informacyjnych* i wprowadzania zmian w już używanych *Systemach informacyjnych*,
- obligatoryjną fazę testowania przed dopuszczeniem nowego *Systemu informacyjnego* i rozdzielenia środowisk testowych oraz produkcyjnych,
- zapewnienie sporządzenia i aktualizacji dokumentacji *Systemów informacyjnych*,
- nadzorowanie dostępu do kodów źródłowych oprogramowania,
- wdrożone procedury kontroli zmian i aktualizacji oprogramowania.

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera **procedura PZ-ZI-05 - „Bezpieczeństwo teleinformatyczne”, procedura PZ-ZI-10 – „Organizacja procesów bezpieczeństwa teleinformatycznego w systemach informacyjnych”** oraz **instrukcja IO-AIT-03 - „Systemy gromadzenia danych i przetwarzania informacji w UCK – nadzór nad rozwojem lub zmianą systemów informacyjnych oraz zasady dopuszczania ich do używania”**.

21. Zarządzanie ciągłością działania

UCK podejmuje działania w zakresie zapewnienia ciągłości funkcjonowania usług związanych z *Przetwarzaniem informacji* w celu przeciwdziałania przerwom w działalności statutowej UCK związanej z *Przetwarzaniem informacji* oraz w celu ochrony kluczowych *Procesów* lub *Systemów informacyjnych* przed zdarzeniami, które mogą zakłócić ich przebieg lub osiąganie założonych wyników. UCK uwzględnia w tych działaniach zapewnienie ciągłości *Procesów* bezpieczeństwa wynikających z *SZBI*. Działania te są realizowane zgodnie z zasadami określonymi w UCK dla *Systemu Zarządzania Ciągłością Działania* określonych w **dokumencie KJ-DZ 23.0 – „Polityka zarządzania ciągłością działania”** oraz **procedurze PZ-08 – „Zarządzanie ciągłością działania UCK”**.

Skuteczna realizacja postawionego celu możliwa jest dzięki utrwalonym praktykom i podziałowi odpowiedzialności związanemu z *Zarządzeniem ciągłością działania* w taki sposób, aby zapobiegać wystąpieniu zdarzeń, które mogą zakłócić ciągłość *Procesów* UCK oraz ograniczać do akceptowalnego poziomu skutki ewentualnych *Incydentów*.

Na wypadek katastrofy lub rozległej awarii technicznej są opracowane, wdrażane oraz okresowo testowane i aktualizowane *Plany ciągłości działania* (*PCD*) dla *Kluczowych systemów informacyjnych* i innych *Systemów informacyjnych* istotnych z punktu widzenia działalności statutowej UCK, zapewniające *Dostępność Informacji* na wymaganym poziomie i w wymaganym czasie po wystąpieniu przerwy lub awarii krytycznych *Procesów* statutowych.

Zespół ds. bezpieczeństwa informacji dba o aktualność *Planów ciągłości działania* i testuje je pod względem przydatności w sytuacji realnego *Zagrożenia*. Analizuje okresowo zdarzenia, które mogą mieć wpływ na *Ciągłość działania*, a w przypadku istotnych zdarzeń wprowadzane są zmiany w *PCD*. Powyższe zasady zapewniają, że UCK jest przygotowane na działanie również w przypadkach odbiegających od normy.

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera **procedura PZ-08 - „Zarządzanie ciągłością działania"**.

22. Zarządzanie incydentami i słabościami Systemu Zarządzania Bezpieczeństwem Informacji

Osoba / *Podmiot zewnętrzny* uzyskująca/uzyskujący dostęp do *Zasobów informacyjnych* UCK, w zakresie uzyskanych uprawnień, ma obowiązek informowania o wystąpieniu *Incydentu związanego z bezpieczeństwem informacji* oraz o wszelkich zidentyfikowanych słabościach *SZBI*.

O *Incydencie* należy niezwłocznie poinformować *Właściciela Zasobu* oraz Pełnomocnika DN ds. SZBI, a w przypadku jego nieobecności niezwłocznie powiadomić Dyrektora Naczelnego lub inną osobę – zgodnie ze schematem powiadamiania, o którym mowa w **procedurze PZ-ZI-02 – „Zarządzanie incydentami i słabościami Systemu Zarządzania Bezpieczeństwem Informacji"**.

O innych *Zdarzeniach związanych z bezpieczeństwem informacji* należy poinformować bezpośredniego przełożonego (dotyczy *Pracowników*) oraz właściwą *Komórkę organizacyjną* UCK ustalonymi źródłami komunikacji *ZSZ* lub zgodnie z postanowieniami umownymi.

UCK na bieżąco monitoruje *Systemy informacyjne* w celu wykrywania zakłóceń w ich funkcjonowaniu lub *Podatności* na *Zagrożenia cyberbezpieczeństwa.*

W przypadku wystąpienia *Incydentu* niezwłocznie podejmuje się działania mające na celu zmniejszenie potencjalnych strat i zapobieżenie rozprzestrzeniania się tego *Incydentu*, a następnie należy go szczegółowo przeanalizować i podjąć decyzje na temat dalszego postępowania. *Incydenty związane z bezpieczeństwem informacji* winny być rejestrowane w taki sposób, żeby można było wyodrębnić z nich *Incydenty cyberbezpieczeństwa.*

UCK zapewnia, żeby wnioski z obsługi *Incydentów* były uwzględniane przy projektowaniu nowych *Procesów*, *Systemów informacyjnych* i *Zabezpieczeń.*

Szczegółowe postanowienia odnoszące się do podejmowanych w ramach tego obszaru działań zawiera **procedura PS-07 - „Nadzór nad niezgodnościami"** oraz **procedura PZ-ZI-02 - „Zarządzanie incydentami i słabościami Systemu Zarządzania Bezpieczeństwem Informacji"**, a także **procedura PZ-ZI-10 - „Organizacja procesów zarządzania bezpieczeństwem teleinformatycznym w systemach informacyjnych".**

23. Zgodność z wymaganiami prawnymi i innymi

W celu uniknięcia naruszeń przepisów prawa powszechnie obowiązującego, w tym w szczególności przepisów prawa karnego, cywilnego oraz innych ustaw, a także rozporządzeń, umów oraz jakichkolwiek wymagań bezpieczeństwa, UCK dba o zapewnienie zgodności zasad postępowania z przepisami prawa powszechnie obowiązującego, przyjętymi normami, postanowieniami umownymi, standardami i innymi regulacjami.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z:

- prowadzeniem monitorowania i przeglądów *SZBI*,
- identyfikacją, monitorowaniem i aktualizacją wymagań prawa powszechnie obowiązującego i innych wymagań w zakresie *Bezpieczeństwa informacji*, a w szczególności wymagań dotyczących *Informacji* prawnie chronionych,
- prowadzeniem nadzoru nad komplementarnością i bezpieczeństwem stosowanych technicznych urządzeń wchodzących w zakres *SZBI*,

- opracowywanie i stosowanie ustandaryzowanych wzorów umów zawieranych z *Podmiotami zewnętrznymi* oraz minimalnych wymagań dotyczących parametrów urządzeń lub usług związanych z *Cyberbezpieczeństwem*,
- uwzględnienie w *Procesie* weryfikacji przyjętych zasad *Bezpieczeństwa informacyjnego* osób posiadających odpowiednią wiedzę i kompetencje,
- prowadzeniem audytów wewnętrznych funkcjonowania *SZBI*.

24. Rozpowszechnianie i zarządzanie dokumentem Polityki Bezpieczeństwa Informacji

Niniejszy dokument podlega regularnym przeglądom dokonywanym przez *Zespół ds. bezpieczeństwa informacji* podczas okresowych przeglądów *SZBI*. W zależności od potrzeb mogą zostać przeprowadzone dodatkowe przeglądy (np. w przypadku stwierdzenia istotnego naruszenia bezpieczeństwa lub pojawienia się zasadniczych zmian w UCK, jego strukturze lub otoczeniu, np. nowego *Zagrożenia*, nowej technologii).

Niniejszy dokument oraz dokumentacja z nim związana winny być rozpowszechniane i modyfikowane zgodnie z **procedurą PS-01 – „Nadzór nad dokumentami i przepisami prawnymi".**

Modyfikacje będą dokonywane, w zależności od potrzeb, m.in. na skutek:

- ogłoszenia nowych lub zmian istniejących przepisów prawa powszechnie obowiązującego,
- przekazania uwag przez odbiorców Polityki Bezpieczeństwa Informacji,
- zaleceń poaudytowych,
- przeprowadzenia okresowych przeglądów Polityki Bezpieczeństwa Informacji,
- zmian organizacyjnych w UCK.

25. Postanowienia końcowe

Z treścią niniejszego dokumentu winni zostać zapoznani wszyscy *Pracownicy*, niezależnie od formy prawnej zatrudnienia. Inne osoby lub *Podmioty zewnętrzne,* które mają uzyskać dostęp do *Zasobów informacyjnych* UCK na podstawie umów, porozumień lub innych stosunków prawnych, a zwłaszcza współpracujące z UCK *Podmioty zewnętrzne* (przed ich dopuszczeniem do *Zasobów informacyjnych* UCK) należy zapoznać z jego treścią, na zasadach określonych w ww. dokumencie, nie później niż przed uzyskaniem dostępu do *Zasobów informacyjnych*.

Za złożenie przez ww. osoby stosownych oświadczeń oraz uzyskanie niezbędnych uprawnień dostępowych (do pomieszczeń i *Systemów informacyjnych* UCK), stosownie do przypisanej roli, odpowiada bezpośredni przełożony *Pracownika* lub *Właściciel Zasobu*.

Naruszenie świadome lub przypadkowe postanowień niniejszej Polityki Bezpieczeństwa Informacji lub dokumentacji z nią powiązanej, stanowi podstawę odpowiedzialności przewidzianej w Regulaminie Pracy UCK oraz w innych wewnętrznych regulacjach UCK, odpowiedzialności określonej w umowach cywilnoprawnych, a także odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego.

Podstawą egzekwowania przestrzegania zasad ochrony *Informacji* od innych niż *Pracownicy* osób / *Podmiotów zewnętrznych*, w tym *Podmiotów zewnętrznych* uczestniczących w *Procesach* związanych z działalnością UCK, są przepisy prawa powszechnie obowiązującego oraz zapisy umów/porozumień z tymi osobami / *Podmiotami zewnętrznymi*, zawierające deklarację o zachowaniu *Poufności*, w tym o zachowaniu w *Poufności Informacji* prawnie chronionych, zobowiązanie do działania zgodnie z prawem i niniejszą Polityką, a także – o ile mają zastosowanie – dodatkowe obowiązki odnoszące się do *Bezpieczeństwa informacji*.

Odstępstwo od zasad opisanych w niniejszym dokumencie lub dokumentacji *SZBI* jest możliwe w drodze wyjątku, wyłącznie po uzyskaniu akceptacji Dyrektora Naczelnego. Wniosek do Dyrektora Naczelnego powinien mieć formę pisemną i zawierać opis odstępstwa oraz uzasadnienie jego zastosowania.

Dyrektor Naczelny przed wyrażeniem zgody na odstępstwo dokonuje weryfikacji wpływu odstępstwa na funkcjonowanie *SZBI*. Odstępstwa, które spowodują naruszenie przez UCK obowiązków wynikających z przepisów prawa powszechnie obowiązującego nie uzyskają akceptacji.

Zatwierdził
DYREKTOR NACZELNY
Uniwersyteckie Centrum Kliniczne
Jakub Kraszewski

26. Załączniki

Załącznik nr 1 – „Fazy postępowania. Cykl Deminga"

Załącznik nr 2 - „Informator Bezpieczeństwa Informacji"