

	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	1 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

1. Cel i zakres opracowania Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji (PBI) wyraża wolę *Najwyższego Kierownictwa UCK* w zakresie ochrony jego *Zasobów informacyjnych*, a także wyznacza główne kierunki działania *Kierownictwa* oraz *Pracowników UCK* 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 zapewnienia *Bezpieczeństwa Informacji*, w tym 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

Ileć w dokumencie jest mowa o terminach związanych z funkcjonowaniem *Systemu Zarządzania Bezpieczeństwem Informacji*, należy przez to rozumieć terminy w znaczeniu wskazanym w „**Leksykonie Uniwersyteckiego Centrum Klinicznego**”, a zwłaszcza w znaczeniu odnoszącym się do *SZBI*, który stanowi załącznik nr 10 do *Księgi Zintegrowanego Systemu Zarządzania*.

3. Deklaracja Najwyższego Kierownictwa

Dyrektor Naczelny UCK, 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 ochrony jego *Zasobów informacyjnych*, 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 UCK deklaruje podjęcie działań niezbędnych do zapewnienia pełnego zintegrowania wdrożonego *Systemu Zarządzania Bezpieczeństwem Informacji* z *Systemem Zarządzania Ciągłością Działania* i *Zintegrowanego Systemu Zarządzania* oraz zapewnienia jego zgodności 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 Rzeczypospolitej 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**”.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	2 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

5. Zakres Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

SZBI został opracowany, wdrożony i jest utrzymywany w oparciu o normę PN-EN ISO/IEC 27001, a jego zakres 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.

Zakres *Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)* odnosi się do całej organizacji i wszystkich realizowanych w niej procesów. Oznacza to, że ochrona informacji zgodnie z wdrożonym SZBI, obejmuje:

- wszystkich *Pracowników UCK* (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, na jakim zostały utrwalone,
- *Urządzenia końcowe* i inne urządzenia wykorzystywane przez UCK do *Przetwarzania informacji*, a także inne *Nośniki danych* (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 teleinformatyczne* 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.

Każdy *Pracownik UCK* przed uzyskaniem dostępu do *Zasobów informacyjnych UCK*, zapoznawany jest z zasadami bezpieczeństwa oraz aktualnymi procedurami ochrony *Informacji* w UCK, w tym z zasadami bezpieczeństwa odnoszącymi się do danego stanowiska pracy. Ewentualne odatkowe postanowienia dotyczące ochrony *Informacji* i zachowania ich w *Poufności*, w tym terminów jej zachowania oraz wiążącej się z tym odpowiedzialności, określone 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.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	3 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

W ramach ustanowionego i wdrożonego *Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)* UCK objęło nadzorem wszystkie funkcjonujące i podejmowane przez siebie procesy. Podejście procesowe odzwierciedla zastosowany przez UCK cykl PDCA, zwany również cyklem Deminga. Oparty o cykl PDCA *System Zarządzania Bezpieczeństwem Informacji (SZBI)* pozwala na całościowe i skoordynowane spojrzenie na *Ryzyko* odnoszące się do *Bezpieczeństwa Informacji* oraz wdrożenie kompleksowego zestawu *Zabezpieczeń 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 następujące 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 *Systemu Zarządzania Bezpieczeństwem Informacji* (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 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 bądź przypadkowej działalności człowieka oraz ich ewentualnych skutków,
- *Zarządzanie cyberbezpieczeństwem* w taki sposób, żeby ograniczać liczbę występujących *Incydentów cyberbezpieczeństwa* oraz zapewnić odpowiednią reakcję na *Incydenty poważne cyberbezpieczeństwa*

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	4 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

oraz *Incydenty krytyczne cyberbezpieczeństwa*, która pozwoli na ograniczenie ich skutków oraz prawdopodobieństwa ponownego wystąpienia,

- zapewnienie *Zasobów* niezbędnych do podjęcia działań w sytuacjach zakłócających normalne funkcjonowanie UCK (związanych z zapewnieniem ciągłości UCK),
- przyczynienie się do ochrony interesów UCK, w tym utrzymania jego dobrego wizerunku, jako organizacji dbającej o *Bezpieczeństwo informacji*, a tym samym wpłyniecie 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 oraz odpowiednie ich zabezpieczenie,
- określanie szans oraz *Zarządzanie ryzykiem*, na które składa się:
 - *Identyfikacja ryzyka*
 - *Estymacja ryzyka*,
 - *Ocena ryzyka*,
 - określenie *Planu Postępowania z Ryzykiem*,
 - proces *Postępowania z ryzykiem* (wdrożenie ustalonych w Planie środków modyfikujących *Ryzyko*),
 - akceptacja *Ryzyk szczytkowych*,
- *Zarządzanie zmianami*, na które składa się:
 - analiza wpływu zmian na poziom *Bezpieczeństwa informacji*,
 - zapewnienie pełnej koordynacji procesu wprowadzania zmian,

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	5 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

- *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 dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na *Zagrożenia* i *Incydenty*,
- prowadzenie działań zmierzających do poprawy poziomu *Bezpieczeństwa informacji*, w tym ciągłe doskonalenie *Systemu Zarządzania Bezpieczeństwem Informacji* zgodnie z wymaganiami normy PN-EN ISO/IEC 27001 i zaleceniami *Zainteresowanych stron*.

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

- firmami 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 Urzędem Ochrony Danych Osobowych oraz Ministrem właściwym ds. Cyfryzacji oraz organami właściwymi ds. *Cyberbezpieczeństwa*,
- pozostałymi podmiotami i instytucjami (m.in. klientami indywidualnymi i instytucjonalnymi, dostawcami, partnerami branżowymi i innymi *Zainteresowanymi stronami*).

8. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji

Dokumentacja *Systemu Zarządzania Bezpieczeństwem Informacji* (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 *Systemu Zarządzania Bezpieczeństwem Informacji* (SZBI), w tym wszelkich działań związanych z ochroną *Informacji*.
- zapewnienia poziomu *Bezpieczeństwa informacji*, który spełnia wymagania określone w obowiązujących przepisach prawa 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 systemu 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,

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	6 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

- przekazania *Podmiotom zewnętrznym* współpracującym z UCK na podstawie umów, porozumień lub innych stosunków prawnych obowiązujących w UCK zasad ochrony,
- zachowania należytej dbałości o *Poufność, Integralność i Dostępność Informacji* podczas kontaktów z pacjentami, *Klientami*, instytucjami i innymi podmiotami współpracującymi.

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”,
- 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 mają moc nadrzędną nad zapisami wdrożonego w UCK Systemu Zarządzania Bezpieczeństwem Informacji, w tym zapisami niniejszej Polityki Bezpieczeństwa Informacji oraz wynikającymi z niej dokumentów podrzędnych.

Polityka Bezpieczeństwa Informacji (PBI) jest dokumentem nadrzędnym nad wszystkimi innymi dokumentami dotyczącymi *Bezpieczeństwa informacji*, wchodzącymi w zakres SZBI. Wszystkie dokumenty związane z *Bezpieczeństwem informacji* są podporządkowane niniejszej Polityce. Zasady określone w dokumentach SZBI należących do kolejnych poziomów nie mogą pozostawać w sprzeczności z treścią dokumentów z poziomów nadrzędnych.

Rozwiązywanie ewentualnej kolizji treści dokumentów wchodzących w zakres SZBI leży w kompetencjach Pełnomocnika Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji.

Rozwiązywanie ewentualnej kolizji PBI z pozostałą dokumentacją ZSZ leży w kompetencjach właściwej merytorycznie *Komórki organizacyjnej* UCK / *Właściciela Zasobu* przy współpracy z Pełnomocnikiem Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji oraz Pełnomocnikiem Dyrektora Naczelnego ds. Systemu Zarządzania.

9. Struktura zarządzania bezpieczeństwem informacji i podział odpowiedzialności

9.1. Poziomy działań

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.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	7 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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*), 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 teleinformatycznych* oraz przestrzegania w praktyce używania tych rozwiązań i systemów (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.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	8 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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 oraz wyznaczeni do nadzorowania PBI *Pracownicy* UCK realizują obowiązki związane z utrzymaniem *Bezpieczeństwa informacji*, w ramach których podejmują działania związane z nadzorem i kontrolą przestrzegania PBI. Od tych *Pracowników* wymagana jest szczególna lojalność, staranność oraz wysoka etyka zawodowa.

Kierownicy komórek organizacyjnych 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 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 swoich podwładnych, 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 tajemnicy podlegającej ochronie *Informacji*, do których uzyskują 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,
- dołożenia wszelkich starań, aby chronić powierzone im i używane przez nich *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:
 - zgłaszanie propozycji zmian w procesie, zarządzaniu, procedurze lub innym dokumencie,

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	9 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

- przekazywania informacji o jakie zwracają się osoby odpowiedzialne za zapewnienie *Bezpieczeństwa teleinformatycznego*, w szczególności Pełnomocnik DN ds. SZBI, Pełnomocnik DN ds. SZ, Kierownik Działu Teleinformatyki, Dyrektorzy Pionów i Kierownicy *Komórek organizacyjnych*,
- uczestnictwo w przeprowadzanych przez UCK szkoleniach z zakresu SZBI.

O każdym *Incydencie* należy niezwłocznie poinformować *Właściciela Zasobu* oraz Pełnomocnika Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji, a w przypadku jego nieobecności niezwłocznie powiadomić Dyrektora Naczelnego UCK bądź 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* oraz właściwą *Komórkę organizacyjną* UCK w sposób określony w ww. procedurze. 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 dokumentach *SZBI* zgłaszane są do Pełnomocnika Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji, który podejmuje współpracę z Pełnomocnikiem ds. Systemu Zarządzania i/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 *Aktywowi* poprzez regulacje wewnętrzne UCK, w tym za współpracowanie z Zespołem w zakresie *Szacowania ryzyka*, utworzenie *Planu postępowania z ryzykiem*, dobór zabezpieczeń oraz *Plan ciągłości działania*, nawet w przypadku, gdy za bieżące utrzymywanie *Aktywu* odpowiada *Podmiot zewnętrzny*.

Właściciel zasobu (Właściciel aktywu) odpowiedzialny jest również za:

- udostępnienie Pełnomocnikowi Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji oraz Zespołowi ds. Bezpieczeństwa Informacji wszelkich danych i *Informacji* 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 Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	10 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

Administrator zasobu teleinformatycznego (*Administrator Systemu*) jest odpowiedzialny za nadzorowanie bezpiecznej eksploatacji i utrzymania oddanego mu do administrowania *Systemu teleinformatycznego* 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 tego systemu, dokonywanie ich przeglądu, zapewnienie aktualności i *Rozliczalności*,
- dokonywanie aktualizacji ww. systemu oraz wsparcie działań związanych z jego rozwojem,
- współpracowanie z dostawcą ww. systemu,
- współpracowanie z Pełnomocnikiem Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji, Pełnomocnikiem Dyrektora Naczelnego ds. Systemu Zarządzania oraz innymi osobami przy opracowaniu projektów procedur, instrukcji oraz dokumentacji wykonawczej lub zmian w ww. dokumentacji odnoszących się do zarządzania ww. systemem,
- udzielanie pomocy technicznej dla *Użytkowników* ww. systemu,
- sporządzanie dotyczącej ww. systemu 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 Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji:

- pełni rolę osoby nadzorującej z upoważnienia *Administradora Danych Osobowych* przestrzeganie w UCK stosowania *Środków technicznych* i *Środków organizacyjnych* zapewniających ochronę przetwarzanych *Danych osobowych* w sposób odpowiedni do *Zagrożeń* oraz kategorii danych objętych ochroną,
- koordynuje opracowanie i wdrożenie zmian oraz doskonalenie *Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)* oraz związanych z nim polityk, procedur, metodyk *Szacowania ryzyka* i mierników poziomu zabezpieczeń dla systemu, 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:

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	11 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

- 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 UCK 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 teleinformatycznych UCK*,
 - zapewnienia zgodności procesu *Zarządzania incydentami 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 służących do *Przetwarzania informacji* oraz *Zabezpieczeń* rekomendowanych przez Zespół ds. Bezpieczeństwa Informacji,
- decyduje o współpracy w zakresie *Bezpieczeństwa informacji* z innymi podmiotami,
- wyraża zgodę na udostępnienie stronom trzecim *Informacji* stanowiących *Tajemnicę UCK*.

9.7. Zespół ds. Bezpieczeństwa Informacji

W skład Zespołu ds. Bezpieczeństwa Informacji (Zespół) wchodzi:

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	12 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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

Zespół okresowo, stosownie do potrzeb, zwoływany jest przez Pełnomocnika Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji w porozumieniu z Dyrektorem Naczelnym UCK.

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 *Bezpieczeństwem informacji*.

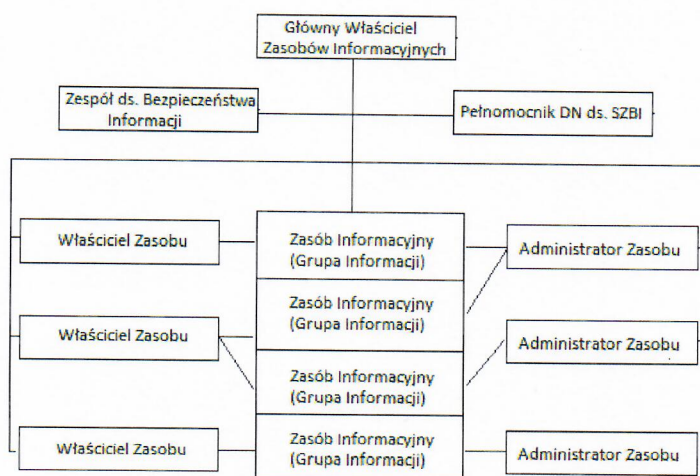
Do zadań Zespołu ds. Bezpieczeństwa Informacji należy:

- dokonywanie okresowego przeglądu Polityki Bezpieczeństwa Informacji oraz pozostałych dokumentów SZBI,
- uzgadnianie ogólnego podziału odpowiedzialności za *Bezpieczeństwo informacji* w odniesieniu do wszystkich obszarów działalności UCK,
- uzgadnianie przedstawionej przez Pełnomocnika 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*, 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*,

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	13 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

- koordynacja procesów doskonalenia SZBI, w tym wdrażania określonych *Zabezpieczeń* w systemach, procesach lub usługach,
- zabezpieczanie realizacji Polityki Bezpieczeństwa Informacji w UCK,
- zgłaszanie do Pełnomocnika Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji poprawek i aktualizacji do opracowywanych dokumentów SZBI, w tym do 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 *System Zarządzania Bezpieczeństwem Informacji (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 UCK, 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 – ulepszone w taki sposób, aby:

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	14 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

- 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* UCK, 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.

Szczegółowe zasady ochrony *Informacji* przetwarzanych w ramach prowadzonej przez UCK działalności, dla każdej z dziedzin bezpieczeństwa, określają – ustanowione na podstawie niniejszej Polityki Bezpieczeństwa Informacji – pozostałe procedury i instrukcje wchodzące w zakres *SZBI*, a także zarządzenia i 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 informacyjnych*, a w zakresie właściwego używania *Pracownicy* lub *Podmioty zewnętrzne*, którym UCK powierzyło je do wykorzystywania 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 *System Zarządzania Bezpieczeństwa Informacji*.

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

W celu ograniczenia ryzyka błędu, kradzieży, nadużycia lub niewłaściwego użytkowania *Zasobów* UCK dba o zapewnienie kompetentnych osób do realizacji wyznaczonych w procesach zadań.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	15 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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 dotyczące *Bezpieczeństwa informacji* oraz ochrony *Zasobów UCK* w ramach wdrożonego 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 trzech podstawowych aspektów *Bezpieczeństwa informacji* – *Poufności*, *Dostępności* i *Integralności*.

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 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 UCK*.

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”**.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	16 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

14. Zarządzanie bezpieczeństwem systemów i sieci

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

- kompetencjom i świadomości *Pracowników* oraz podpisanym umowom ze specjalistycznymi firmami administrującymi *Systemami informacyjnymi* i wspomagającymi UCK,
- opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy,
- nadzorowaniu wprowadzania zmian do infrastruktury technicznej,
- w celu zapewnienia bezpieczeństwa systemów produkcyjnych, prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach,
- nadzorowaniu usług dostarczanych przez strony trzecie, a w szczególności wszelkich wprowadzanych zmian do systemów (dostarczane usługi i wprowadzane zmiany winny być odbierane i akceptowane w sposób świadomy, przy uwzględnieniu ich wpływu na istniejący system bezpieczeństwa),
- wdrożeniu *Zabezpieczeń* chroniących przed złośliwym i/lub szkodliwym oprogramowaniem,
- systematycznemu tworzeniu i testowaniu *Kopii bezpieczeństwa*,
- przestrzeganiu opracowanych zasad postępowania z nośnikami,
- bieżącym monitorowaniu *Aktywów informacyjnych* pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów,
- monitorowaniu poziomu *Incydentów* w *Systemach informacyjnych* i wdrożeniu mechanizmów reagowania w sytuacji ich wystąpienia.

Wszystkie informacje, które nie stanowią informacji publicznych, 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, zgodnie z najnowszym stanem wiedzy i zaleceniami zawartymi w normie PN-EN ISO 27002:2017. 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 planów działania 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,

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	17 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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

15. Autoryzacja nowych urządzeń, eksploatacja i utrzymanie zasobów informacji

Każde nowe lub zmienione urządzenie służące do *Przetwarzania informacji* lub inny *Aktyw* mogący w jakikolwiek inny sposób wpływać na *Bezpieczeństwo informacji* muszą zostać zweryfikowane na zgodność z wymaganiami *Systemu Zarządzania Bezpieczeństwem Informacji* 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*. 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) wykonywane są przez *Administradora*.

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

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	18 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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 wymaganych dokumentów odnoszących się do zachowania *Poufności*, w tym do zachowania w tajemnicy *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 uzupełniających ją dokumentów 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 tajemnicy *Informacji* prawnie chronionych oraz zobowiązania do działania zgodnie z prawem, winny określać – o ile mają zastosowanie - obowiązujące te podmioty/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*, z którym winny być zgodne wszelkie ewentualne dodatkowe postanowienia umowne, zawiera **ogólnodostępny „Informator bezpieczeństwa informacji” - Załącznik nr 2 do niniejszej Polityki**, który został również umieszczony na ogólnodostępnej stronie 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 pod adresem <https://uck.pl/nasz-szpital/bezpieczenstwo-informacji/podstawowe-informacje.html>

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	19 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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 zakłócenia spokoju i porządku publicznego następuje poprzez:

- udzielanie wzajemnej pomocy w realizacji zadań ochrony i zapobieganiu przestępczości,
- udzielanie wyczerpujących informacji o zagrożeniu 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/podmiot zawiadamia Straż Pożarną oraz Dyrektora Naczelnego UCK. Przybyłe jednostki ratownicze natychmiast kieruje się na miejsce akcji.

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”**.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	20 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

19. Kontrola dostępu

W celu zapewnienia, że dostęp do *Informacji*, miejsc, urządzeń lub systemów ich przetwarzania mają tylko osoby uprawnione, 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. Pozyskanie, rozwój i utrzymanie zasobów informacyjnych

Wszystkie procesy związane z pozyskaniem, rozwojem bądź 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:

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

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	21 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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 danych i 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 osiągnięcie 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 ciągłości działania* w taki sposób, aby zapobiegać wystąpieniu *Zdarzeń*, które mogą zakłócić ciągłość procesów w 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* 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 *Planach ciągłości działania*. 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

Każda osoba/podmiot uzyskująca 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 Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwem Informacji, a w przypadku jego nieobecności niezwłocznie powiadomić Dyrektora Naczelnego UCK lub inną osobę – zgodnie ze schematem powiadamiania, o którym mowa w **procedurze PZ-ZI-02 – „Zarządzanie incydentami i słabościami Systemu Zarządzania Bezpieczeństwem Informacji”**.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	22 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

O innych *Zdarzeniach związanych z bezpieczeństwem informacji* należy poinformować bezpośredniego przełożonego (dotyczy *Pracowników UCK*) oraz właściwą *Komórkę organizacyjną* UCK ustalonymi źródłami komunikacji Zintegrowanego Systemu Zarządzania 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, 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 prawnych i innych w zakresie *Bezpieczeństwa informacji*, a w szczególności wymagań dotyczących informacji prawnie chronionych,
- prowadzeniem nadzoru nad komplementarnością i bezpieczeństwem stosowanych technicznych urządzeń wchodzących w zakres Systemu Zarządzania Bezpieczeństwem Informacji,
- opracowywanie i stosowanie ustandaryzowanych wzorów umów zawieranych z *Podmiotami zewnętrznymi* oraz wymogów minimalnych 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*.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	23 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

24. Rozpowszechnianie i zarządzanie dokumentem Polityki Bezpieczeństwa Informacji

Niniejszy dokument podlega regularnym przeglądom dokonywanym przez Zespół ds. Bezpieczeństwa Informacji podczas okresowych przeglądów *Systemu Zarządzania Bezpieczeństwem Informacji*. 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 dokumenty z nim związane 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,
- 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* UCK, niezależnie od formy prawnej zatrudnienia. W stosunku do innych osób lub podmiotów, 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) – powinni zostać zapoznani na zasadach określonych w takim dokumencie, nie później niż przed uzyskaniem dostępu do *Zasobów informacyjnych*.

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

Naruszenie świadome bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji, a także dokumentów powiązanych, 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, w tym *Podmiotów zewnętrznych* uczestniczących w procesach związanych z działalnością UCK, są przepisy prawa oraz zapisy umów/porozumień z tymi osobami/podmiotami, zawierające deklarację o zachowaniu *Poufności*, w tym o zachowaniu w tajemnicy *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*.

 Uniwersyteckie Centrum Kliniczne	Egzemplarz	1
	Rozdział	KJ-Dz.21.0
KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Edycja	6
	Strona/ stron	24 z 24
POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data edycji rozdziału	22.03.2023

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

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

Zaakceptował

DYREKTOR NACZELNY
Uniwersyteckie Centrum Kliniczne

Jakub Kraszewski

26. Załączniki

Załącznik nr 1 – „Fazy postępowania. Cykl Deminga”

Załącznik nr 2 - „Informator Bezpieczeństwa Informacji”