Spis treści:

Cel i zakres

- Celem dokumentu jest określenie zasad zapewnienia bezpieczeństwa informacji w Powiatowym Centrum Zdrowia Sp. z o. o. Celem jest przeciwdziałanie potencjalnym zagrożeniom oraz minimalizacja skutków naruszenia bezpieczeństwa informacji oraz przedstawienie obowiązujących podstawowych zasad ustanowionych w celu zapewnienia bezpieczeństwa przetwarzanych *Informacji*, w tym zapewniania ich *Poufności, Integralności, Dostępności i Autentyczności*.
- Polityka Bezpieczeństwa Informacji oraz regulacje z niej wynikające obowiązują wszystkich pracowników i współpracowników oraz inne osoby uzyskujące dostęp do informacji przetwarzanych w Powiatowym Centrum Zdrowia Sp. z o. o. na zasadach współpracy (z wyłączeniem osób uzyskujących dostęp na podstawie szczególnych przepisów prawa w zakresie ich obowiązywania).

Postanowienia ogólne

- Najwyższe kierownictwo Powiatowego Centrum Zdrowia Sp. z o. o. rozumiejąc konieczność zapewnienia odpowiedniego poziomu ochrony informacji w świadczonych usługach, a także w celu spełnienia wymagań prawnych w odniesieniu do ochrony informacji, ustanawia System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz opiera się na normie PN-ENISO/ICE 27001, którego nadrzędny dokument stanowi niniejsza Polityka Bezpieczeństwa Informacji.
- Głównym celem wdrożenia SZBI jest odpowiednie zabezpieczenie przetwarzanych w Powiatowym Centrum Zdrowia Sp. z o. o. informacji z zachowaniem ich poufności, dostępności i integralności.
- Poufność informacji oznacza, że jest ona dostępna wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji.
- Dostępność informacji oznacza możliwość wykorzystania informacji przez upoważnioną osobę na każde uzasadnione żądanie w ustalonym czasie.
- Integralność informacji oznacza, że informacja nie uległa zmianie od czasu ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób.
- Powyższy cel osiągany jest poprzez:

- określenie przez Najwyższe kierownictwo Powiatowego Centrum Zdrowia Sp. z o. o. kierunków rozwoju zarządzania bezpieczeństwem informacji;
- zapewnienie odpowiedniego zaangażowania pracowników w utrzymanie bezpieczeństwa informacji;
- spełnienie wszelkich wymogów obowiązującego prawa odnośnie ochrony przetwarzanych informacji;
- zarządzanie ryzykiem w obszarze bezpieczeństwa informacji;
- wdrażanie zabezpieczeń adekwatnych do wyników analizy ryzyka, chroniących przed utratą bezpieczeństwa informacji ze szczególnym uwzględnieniem poufności, dostępności i integralności informacji i środków ich przetwarzania;
- ciągłe doskonalenie wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji oraz podjęcie niezbędnych działań do zapewnienia pełnego zintegrowania z Zintegrowanym Systemem Zarządzania;
- zapewnienie zgodności z celami i planami strategicznymi na dany rok, jak i długofalowym Planem Strategicznym PCZ sp. z o.o.
- Najwyższe kierownictwo Powiatowego Centrum Zdrowia Sp. z o. o. – rozumiejąc konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa – deklaruje pełne wsparcie dla podejmowanych działań w zakresie bezpieczeństwa informacji oraz zapewnienie niezbędnych zasobów i czasu na ich realizację, której dowodem jest Deklaracja Polityki Bezpieczeństwa Informacji, stanowiąca załącznik do Księgi Zintegrowanego Systemu Zarządzania, zgodnie z uwarunkowaniami prawnymi określonymi w niniejszym dokumencie.

Podstawowe definicje i skróty

- Pojęcia używane w dokumentacji SZBI są zdefiniowane w ISO/IEC 27000, ISO 22301 oraz przepisach prawa (w tym w ustawie KSC),
- PCZ – Powiatowe Centrum Zdrowia sp. z o.o. z siedzibą w Kartuzach,
- SZBI – System Zarządzania Bezpieczeństwem Informacji w PCZ.

Zakres systemu Zarządzania Bezpieczeństwem Informacji

- System Zarządzania Bezpieczeństwem Informacji z poszczególnymi Procesami i interakcjami między mini 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 ustanowiono zakres:
  - *Kontekst wewnętrzny* oraz *Kontekst Zewnętrzny* w jakim funkcjonuje PCZ, w tym czynniki wewnętrze i wewnętrzne, które są istotne dla celu jego działania oraz takie, które wpływają na zdolność spółki do osiągnięcia zamierzonych wyników działania.
  - istotne dla SZBI Strony Zainteresowane oraz ich wymagania, obejmujące w szczególności uwzględnione w ramach SZBI wymagania wynikające z przepisów prawa powszechnie obowiązującego, wymagania regulacyjne, zobowiązania umowne oraz zależności między działaniami realizowanymi przez spółkę oraz *Podmioty zewnętrzne*.
- Zakres SZBI jest właściwy dla prowadzonej przez PCZ działalności, dotyczy: Procesów związanych z udzielaniem świadczeń zdrowotnych, w tym m.in. w zakresie diagnostyki, leczenia stacjonarnego, ambulatoryjnego, medycyny ratunkowej, a także obrotu i dystrybucji produktów leczniczych przez Aptekę Szpitalna oraz przygotowywania, przetwarzania, handlowania i oferowania sprzedaży produktów żywnościowych przez Dział Żywienia. SZBI obowiązuje w całej organizacji i wszystkich realizowanych Procesach.

Role i odpowiedzialność

- Najwyższe kierownictwo PCZ (Właściciel zasobu/ Właściciel Aktywu) odpowiada za:
  - zarządzanie *Aktywem* tj. utrzymanie wyznaczonego poziomu powierzonego mu *Aktywu* poprzez regulacje wewnętrzne spółki oraz współpracowanie z Zespołem ds. cyberbezpieczeńsytwa informacji, w zakresie *Szacowania ryzyka*, utrzymania *Planu postępowania z ryzykiem*, dobór zabezpieczeń oraz *Planu ciągłości* działania również w przypadku, gdy za utrzymanie odpowiada *Podmiot zewnętrzny;*

- zatwierdzanie wyników szacowania ryzyka i planów postępowania z ryzykiem, procedur postepowania;
- informowanie o poziomie Bezpieczeństwa informacyjnego w zakresie przypisanego mu Zasobu (Aktywu);
- powołanie osób do ról w SZBI;
- dokonanie przeglądu SZBI;

– Zespół Cyberbezpieczeństwa odpowiada za:
- systematyczne szacowanie ryzyka dla Systemów Informacyjnych służących do świadczenia Usługi Kluczowej,
- nadzór nad funkcjonowaniem wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji dla Usługi Kluczowej,
- nadzór nad funkcjonowaniem Systemu Zarządzania Ciągłością Działania dla procesu reagowania na incydenty poważne w Systemach Informacyjnych służących do świadczenia Usługi Kluczowej,
- zarządzanie incydentami poważnymi w Systemach Informacyjnych służących do świadczenia Usługi Kluczowej,
- koordynowanie szkoleń w zakresie cyberbezpieczeństwa świadczonej Usługi Kluczowej,
- prowadzenie kampanii informacyjnych z zakresu cyberbezpieczeństwa dla użytkowników Usługi Kluczowej,
- nadzór nad dokumentacją dotyczącą cyberbezpieczeństwa Systemów Informacyjnych służących do świadczenia Usługi Kluczowej,
- koordynowanie audytów cyberbezpieczeństwa Systemów Informacyjnych wykorzystywanych do świadczenia Usługi Kluczowej.

– Pełnomocnik ds. Cyberbezpieczeństwa odpowiada za:
- nadzór nad prawidłową realizacją procesów SZBI,
- nadzoruje przestrzeganie Polityki Bezpieczeństwa Informacji oraz dokumentacji z nią związanej,
- współdziała z Administratorami systemów,

- zarządzanie przeglądem SZBI we współpracy z pełnomocnikiem SZJ,
- prezentację wyników przeglądu SZBI we współpracy z pełnomocnikiem SZJ,
- koordynowanie działań związanych z audytami SZBI we współpracy z pełnomocnikiem SZJ,
- zainicjowanie okresowej analizy ryzyka we współpracy z pełnomocnikiem SZJ i IOD,
- koordynowanie działań związanych z incydentami bezpieczeństwa informacji (w tym cyberbezpieczeństwa) i informowaniu o ich wystąpieniu,
- dokonywanie okresowych przeglądów stanu bezpieczeństwa informacji oraz zgodności z przyjętymi standardami bezpieczeństwa,
- zatwierdzanie zmian w SZBI we współpracy z pełnomocnikiem SZJ,
- nadzór nad udokumentowaną informacją we współpracy z pełnomocnikiem SZJ,
- zatwierdzenie finalnej wersji dokumentacji SZBI,
- zarządzanie Zespołem Cyberbezpieczeństwa,
- reagowanie na nowe sytuacje w zakresie SZBI,
- zatwierdzanie propozycji działań doskonalących w zakresie SZBI we współpracy z pełnomocnikiem SZJ.

– Administrator zasobu (aktywu)-zespół IT odpowiada za**:**

- zarządzanie systemem IT z pozycji uprawnień administracyjnych,
- zapewnia zgodność systemu IT z wymogami prawnymi oraz wewnętrznymi regulacjami bezpieczeństwa,
- konfiguruje systemy IT w sposób zapewniający maksymalny poziom ich bezpieczeństwa,
- dokumentuje czynności wykonywane z pozycji uprawnień administracyjnych,
- nadaje, modyfikuje, zawiesza i odbiera uprawnienia dostępu do systemu IT zgodnie z właściwymi wnioskami,
- przeprowadza okresowe przeglądy uprawnień dostępu do systemie IT,
- zbiera informacje o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu IT,

- systematycznie przegląda logi systemowe, podejmując właściwe reakcje na stwierdzone zdarzenia niepożądane,
- nadzoruje działania podejmowane z kont uprzywilejowanych.

– Inspektor Ochrony Danych odpowiada za**:**
- realizacja procesu zarządzania ryzykiem w zakresie RODO,
- zgłaszanie naruszeń do Urzędu Ochrony Danych Osobowych i informowanie Podmiotu Danych,
- szczegółowy zakres odpowiedzialności IOD został opisany w Polityce Ochrony Danych Osobowych.

– Kadra kierownicza odpowiada za**:**
- koordynowanie opracowywania propozycji działań doskonalących w podległej komórce,
- nadzór nad udokumentowaną informacją SZBI w podległej komórce,
- przestrzeganie zasad bezpieczeństwa informacji przez nich samych jak i przez podległych im pracowników oraz zapewnienie zgodności z wymaganiami przepisów praw powszechnie obowiązujących oraz innych regulacyjnych, w tym z wymaganiami normy PN-EN ISO/ICE27001,
- identyfikowanie i dokumentowanie zagrożeń istotnych dla bezpieczeństwa informacji lub cyberbezpieczeństwa,
- szkolenie instruktażowe pracowników w zakresie związanym z bezpieczeństwem informacji oraz cyberbezpieczeństwem na stanowiskach pracy.

– Audytor wewnętrzny odpowiada za**:**
- przeprowadzanie wspólnych audytów SZBI i SZJ,
- opracowanie raportów z przeprowadzanych audytów i przedstawienie ich Pełnomocnikowi ds. Cyberbezpieczeństwa i SZJ.

– Pracownicy i Współpracownicy odpowiadają za**:**
- przestrzeganie zasad bezpieczeństwa informacji;
- zgłaszanie potencjalnych incydentów bezpieczeństwa informacji;
- zgłaszanie ryzyka bezpieczeństwa informacji;

- realizacji obowiązków służbowych zgodnie z obowiązującymi przepisami prawa powszechnie obowiązujących oraz innych regulacyjnych, w tym z wymaganiami normy PN-EN ISO/ICE27001

Zgodność z wymaganiami prawa i umownymi

– PCZ systematycznie monitoruje ryzyka związane z brakiem zgodności, tj. niedostosowaniem się do przepisów prawa, wymogów organów nadzoru lub też ogólnie przyjętych zasad postępowania i standardów etycznych w działalności PCZ, w relacjach wewnętrznych i zewnętrznych.

– Wszelkie umowy i dokumenty opiniowane są przez Stanowisko ds. obsługi prawnej. Dodatkowo PCZ podlega przepisom ustawy Prawo Zamówień Publicznych.

– W zakresie zgodności działania PCZ z regulacjami prawnymi oraz wymogami organów nadzoru, monitorowanie stanu prawnego oraz jego planowanych zmian, które mogą dotyczyć działalności PCZ realizowane jest w szczególności przez Najwyższe kierownictwo Powiatowego Centrum Zdrowia Sp. z o. o. oraz Stanowisko ds. obsługi prawnej.

Obszary Zarządzania Bezpieczeństwem

W PCZ wydzielono następujące obszary zarządzania bezpieczeństwem informacji:

– Obszar bezpieczeństwa informacji

Obszar obejmuje zasady, procedury i inne regulacje niższego rzędu związane z klasyfikacją informacji i postępowaniem z nią. Szczegółowe regulacje dotyczące tego obszaru zawarte są w dokumencie Polityka Bezpieczeństwa Informacji i dokumentach związanych. Opis zabezpieczeń znajduje się w Deklaracji Stosowania.

– Obszar ochrony danych osobowych

Obszar obejmuje zasady związane wypełnieniem wymagań wynikających z Ustawy o ochronie danych osobowych i RODO. Szczegółowe regulacje dotyczące tego obszaru zawarte są w dokumencie Polityka Bezpieczeństwa Danych Osobowych i dokumentach związanych.

– Obszar zarządzania bezpieczeństwem teleinformatycznym

Obszar obejmuje zasady związane z bezpieczeństwem teleinformatycznym, w tym:

- zasady sporządzania i testowania kopii bezpieczeństwa;
- zasady ochrony przed kodem złośliwym;
- zasady zarządzania systemami informatycznymi i siecią teleinformatyczną;
- zasady używania kryptografii;
- zasady zarządzania kontami i uprawnieniami;
- zasady monitorowania pracy sieci i systemów;
- zasady konserwacji i serwisowania sprzętu teleinformatycznego;
- zasady zarządzania legalnością oprogramowania;
- zasady zarządzania ciągłością działania.

Szczegółowe regulacje dotyczące tego obszaru zawarte są w dokumentach związanych i Zasadach Bezpieczeństwa Teleinformatycznego.

– Obszar zarządzania ryzykiem w bezpieczeństwie informacji

Obszar obejmuje zasady związane z zarządzaniem ryzykiem w bezpieczeństwie informacji. Szczegółowe regulacje dotyczące tego obszaru zawarte są w dokumencie Zarządzanie ryzykiem bezpieczeństwa informacji i cyberbezpieczeństwa oraz dokumentach zastanych.

– Obszar utrzymania SZBI

Obszar obejmuje zasady związane z utrzymaniem SZBI w tym:

- zasady monitorowania skuteczności zabezpieczeń;
- zasady obsługi incydentów (w tym incydentów bezpieczeństwa informacji);
- zasady przeprowadzania przeglądów SZBI;
- zasady nadzoru nad dokumentami i zapisami;
- zasady przeprowadzania działań korygujących i zapobiegawczych;
- zasady przeprowadzania audytów SZBI.

Szczegółowe regulacje dotyczące tego obszaru zawarte są w dokumentacji zintegrowanej z Systemem Zarządzania Jakością.

– Obszar bezpieczeństwa fizycznego

Obszar obejmuje zasady związane zapewnieniem bezpieczeństwa fizycznego aktywów związanych z przetwarzaniem informacji – m.in. zarządzania dostępem do pomieszczeń. Szczegółowe regulacje dotyczące tego obszaru cyberbezpieczeństwa zawarte są w dokumencie Zasady Bezpieczeństwa Fizycznego IT i dokumentach związanych.

– Obszar bezpieczeństwa personalnego

Obszar obejmuje zasady stosowane przez pracowników związane z zapewnieniem bezpieczeństwa informacji. Szczegółowe regulacje dotyczące tego obszaru zawarte są w dokumencie Zasady Bezpieczeństwa Personalnego i dokumentach związanych.

Monitorowanie, pomiary, analiza i ocena

– W PCZ nadzoruje się odpowiednią realizację procedur związanych z incydentami bezpieczeństwa.
– Poprzez audyty wewnętrzne oraz audyty zewnętrzne wykazywany jest faktyczny stan i ocena SZBI.
– Wykonywanie testów bezpieczeństwa pomaga zweryfikować bezpieczeństwo infrastruktury teleinformatycznej i fizycznej.
– Prowadzone jest szacowanie ryzyka umożliwiające identyfikację pojawiających się ryzyk ich odpowiednią ocenę oraz zastosowanie planu postępowania z ryzykami.
– Pomiar skuteczności – jako działania proaktywne umożliwia zweryfikowanie i faktyczną ocenę wprowadzonych zabezpieczeń.

Cele realizowanych procesów

– Celem wdrożonego SZBI jest osiągnięcie poziomu organizacyjnego i technicznego, który:
  - zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych;
  - zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać we wszystkich systemach jej przetwarzania
  - maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę PCZ;

- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji;
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa PCZ, jej interesów oraz posiadanych i powierzonych jej informacji.

– Powyższe cele realizowane są poprzez:

- wyznaczenie osób odpowiedzialnych zapewniających optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji;
- wyznaczenie właścicieli dla kluczowych aktywów przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa;
- zarządzania ryzykiem, na które składa się:
  - Identyfikacja ryzyka,
  - Estymacja ryzyka
  - Ocena ryzyka
  - Określenie Planu postepowania z Ryzykiem;
- zarządzanie Zmianami tj analiza wpływu zmian na poziom Bezpieczeństwa Informacji oraz nadzoru nad Procesami i wprowadzania-aktualizacji zmian;
- zarządzanie Ciągłością działania poprzez wdrożenie procedur i instrukcji awaryjnych celem zapewnienia Ciągłości działania;
- zarządzanie Incydentami naruszającymi bezpieczeństwo informacji oraz słabościami SZBI tj zapewnienie, że wszystkie naruszenia Bezpieczeństwa *Informacji (Incydenty)* oraz jego słabe punkty są raportowane i badane;
- przyjęcie za obowiązujące przez wszystkich pracowników polityk i procedur bezpieczeństwa obowiązujących w PCZ;
- określeniu zasad przetwarzania informacji, w tym stref w których może się ono odbywać;
- przegląd i aktualizację polityk i procedur postępowania dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty;
- ciągłe doskonalenie systemu zapewnia bezpieczeństwo informacji funkcjonującego w PCZ, zgodnie z wymaganiami Ustawy o Krajowym Systemie

Cyberbezpieczeństwa, wymaganiami normy PN-EN ISO/IEC 27001 i zaleceniami wszystkich zainteresowanych stron.

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji

– Podstawowym dokumentem jest niniejsza Polityka Bezpieczeństwa Informacji, która została opracowana w celu**:**
  - udokumentowania zasad ochrony Informacji**,** w tym zapewnienia Cyberbezpieczeństwa, wykorzystywanych do przetwarzania *Systemów informacyjnych* potrzebnych do wdrożenia, eksploatacji, przeglądu, monitorowania i doskonalenia SZBI i wszelkimi działaniami związanymi z ochroną Informacji;
  - zapewnienia poziomu *Bezpieczeństwa Informacji* spełniającego wymagania określone w obowiązujących przepisach prawa oraz identyfikacji *Ryzyka* przez *Szacowanie ryzyka;*
  - informowania *Pracowników, Klientów* uzyskujących dostęp do *Zasobów informacyjnych* PCZ oraz *Stron zaineresowanych* świadczonymi usługami o zasadach działania SZBI i wpływu ich działań na spełnienie wymagań obowiązujących przepisów praw jak i zapobiegania popełnianych błędów z tym zakresie**;**
  - uzyskania optymalnej jakości świadczonych usług poprzez Ciągłe doskonalenia skuteczności działania;
  - przekazywania Podmiotom zewnętrznym współpracującym z PCZ sp. z o.o. na podstawie umów, porozumień lub innych obowiązujących stosunków prawnych zasad ochrony *Informacji***,**
  - zachowania należytej dbałości o *Poufność, Integralność, Dostępność i Autentyczność Informacji* podczas kontaktów z Pacjentami, *Klientami* i innymi podmiotami wewnętrznymi współpracującymi ze spółką.

– W skład dokumentacja SZBI wchodzi:
  - Deklaracja Polityki Bezpieczeństwa Informacji
  - Polityka Bezpieczeństwa Informacji
  - Regulamin Organizacja funkcjonowania Zespołu Cyberbezpieczeństwa
  - Procedura zarządzania bezpieczeństwem Informacji
  - Procedura postępowania na wypadek awarii systemu informatycznego

- Zarządzanie Ciągłością Działania
- Zarządzanie ryzykiem BI
- Zarządzanie zabezpieczeniami kryptograficznymi
- Zasady bezpieczeństwa fizycznego IT
- Zasady Bezpieczeństwa Informacji w realizacjach z dostawcami
- Zasady Bezpieczeństwa Personalnego
- Zasady Bezpieczeństwa Teleinformatycznego
- Deklaracja Stosowania

– Procedury i instrukcje bezpieczeństwa określające zasady postepowania wymienione są w załączniku do Księgi Zintegrowanego systemu zarządzania – Wykaz procedur i dokumentów obowiązujących w PCZ sp. z o.o.

Komunikacja wewnętrzna i zewnętrzna

– Komunikacja wewnętrzna:

Na komunikację wewnętrzną składają się m.in. następujące działania:

- spotkania Prezesa Zarządu z Pełnomocnikiem ds. Cyberbezpieczeństwa;
- spotkania Prezesa Zarządu z osobami zarządzającymi oddziałami/jednostkami organizacyjnymi;
- spotkania Prezesa Zarządu z pracownikami;
- współpraca między poszczególnymi pracownikami;
- dystrybucja dokumentacji SZBI
- Podstawowe sposoby komunikacji w Powiatowym Centrum Zdrowia Sp. z o. o. to:
- komunikacja bezpośrednia;
- komunikacja telefoniczna;
- komunikacja pisemna;
- komunikacja elektroniczna.

– Komunikacja zewnętrzna:

Do udzielania informacji o działalności PCZ. stronom zewnętrznym upoważnieni są: Prezes Zarządu lub osoby wyznaczone przez Prezesa Zarządu.

Zapewnienie zasobów

- Najwyższe kierownictwo zapewnia zasoby, udogodnienia i budżet potrzebny do osiągania zdefiniowanych celów – rozwój polityki bezpieczeństwa informacji.
- Własne zasoby ludzkie są monitorowane pod kątem niezbędnych kompetencji i potrzeb szkoleniowych, a realizacja tych potrzeb następuje w oparciu o posiadane środki i wiedzę. Podejmowane jest także sprawdzanie efektywności działań w tym zakresie.
- Zasoby ludzkie, techniczne i inne poddostawców biorących udział w procesie świadczenia usług są monitorowane oraz zarządzane, pod kątem spełnienia wymagań bezpieczeństwa informacji.

Klasyfikacja i ochrona informacji

- Za klasyfikację informacji odpowiada:
  - osoba tworząca informację;
  - osoba, do której skierowana jest informacja z zewnątrz.

  Osoba ta staje się jednocześnie jej właścicielem.
- Klasyfikacja informacji

  Główną zasadą, która obowiązuje przy klasyfikacji informacji jest jej poufność:
  - do informacji w kategorii „Ogólnodostępne” zaliczamy informacje, które mogą być publikowane, w tym:
    - wszystkie informacje o sprawach publicznych, zamieszczana w BIP Powiatowego Centrum Zdrowia Sp. z o. o.,
    - wszystkie informacje tworzone, przekazywane i przetwarzane w PCZ, nieoznaczone, jako należące do osób trzecich i niesklasyfikowane, jako chronione,
    - publikacje na stronie internetowej PCZ,
  - do informacji w kategorii „Chronione” zaliczamy informacje, które są dostępne wewnątrz PCZ i podlegają ograniczeniom w zakresie przetwarzania, w tym:
    - informacje objęte tajemnicą prawnie chronioną w rozumieniu zapisów art. 100 § 2 pkt 5 ustawy z dnia 26.06.1974 r. Kodeks pracy,
    - nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne PCZ lub inne informacje posiadające wartość gospodarczą,

- nieujawnione do wiadomości publicznej informacje udostępniane w trybie i na zasadach określonych w ustawie z dnia 06.09.2001 r. o dostępie do informacji publicznej,
- chronione informacje niejawne, stosownie do postanowień ustawy z dnia 05.08.2010 r. o ochronie informacji niejawnych,
- chronione dane osobowe, stosownie do postanowień Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO), w szczególności: dane osobowe pracowników PCZ, dane osobowe pacjentów, informacje o stanie zdrowia,
- chronione informacje dotyczące pacjentów - stosownie do ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta,
- informacje chronione tajemnicą zawodową, stosownie przepisów regulujących prawa wykonywania zawodu,
- chronione informacje, których obowiązek zachowania tajemnicy wynika z przepisów prawa powszechnie obowiązującego,
- informacje co, do których PCZ podjęło niezbędne działania w celu zachowania ich poufności, a w szczególności: kadrowo-płacowe, finansowo-księgowe, wewnętrzna komunikacja, korespondencja, poczta elektroniczna, kody dostępu i kody użytkownika (loginu i/lub hasła) do systemu informatycznego.

Jeśli osoba odpowiedzialna za klasyfikację informacji nie potrafi przypisać jej do żadnej z powyższych kategorii lub informacja nie występuje w opisie grup, powinna powiadomić o tym fakcie przełożonego i do czasu ustalenia przez niego kategorii przyjąć, że jest to informacja o kategorii „Chronione”.

– Oznaczanie informacji

Informacje nie są dodatkowo oznaczane. Ograniczenie dostępu do informacji z kategorii „Chronione” realizowane jest z wykorzystaniem zastosowanych zabezpieczeń organizacyjnych i technicznych.

– Postępowanie z informacją

- Informacje „Ogólnodostępne”

Wszystkie informacje sklasyfikowane w kategorii „Ogólnodostępne” zarówno w wersji papierowej jak i elektronicznej oraz na nośnikach z wersją elektroniczną mogą być kopiowane, przesyłane, przekazywane w formie ustnej oraz niszczone przez wszystkich pracowników i współpracowników PCZ zgodnie z jej kulturą organizacyjną. Zalecanym miejscem niszczenia dokumentów papierowych są niszczarki. Informacje należące do powyższej kategorii powinny być przechowywane w sposób uporządkowany.

- Informacje „Chronione”

INFORMACJE	**Wersja papierowa**	**Wersja elektroniczna**	**Odpowiedzialny**
Kopiowanie	Za zgodą właściciela informacji		Właściciel lub osoba upoważniona
Przechowywanie	Szafy biurowe zamykane na klucz	Na dyskach lokalnych, cloud i sieciowych w wyznaczonych i zabezpieczonych miejscach	
Przekazywanie w formie papierowej lub elektronicznej	Za potwierdzeniem odbioru	Informacje powinny być zaszyfrowane	
Przekazywanie w formie ustnej lub innej	Zabrania się przekazywania informacji poprzez pocztę głosową, automatyczną sekretarkę, rozmowy w miejscach publicznych. W przypadku wysyłania informacji chronionej przez kanał publiczny należy jak najszybciej skasować konwersację.		
Wynoszenie	Za zgodą przełożonego		
Niszczenie	Wrzucenie do bezpiecznego pojemnika lub w niszczarkach min. Klasy DIN 3	Poprzez usunięcie informacji bez pozostawiania w katalogach pełniących funkcję Kosza w systemie operacyjnym.	Właściciel lub odbiorca

– Zasady ochrony informacji

- w PCZ ochronie podlegają wszelkie informacje, w odniesieniu do których w jakikolwiek sposób została ustalona ochrona, ograniczenie dostępu lub sposobu wykorzystania:
  - na podstawie powszechnie obowiązujących przepisów prawa;
  - na podstawie decyzji przełożonego;
  - na żądanie kontrahenta (klienta lub dostawcy).
- informacjami podlegającymi „ochronie", są wszelkie informacje przekazywane ustnie lub utrwalone na dowolnych nośnikach, jakich ujawnienie mogłoby narazić PCZ na szkodę. W szczególności są to informacje: kadrowe, finansowe, kontraktowe, zawierające dane osobowe pracowników i pacjentów, itp. Powinnością każdego pracownika jest powstrzymanie się przed ujawnieniem osobie nieuprawnionej informacji chronionej, uzyskanej w związku z zatrudnieniem w PCZ.
- wytwarzanie, przetwarzanie i przekazywanie „chronionych" informacji jest dopuszczalne tylko w warunkach uniemożliwiających ich nieuprawnione ujawnienie.
- informacje podlegające ochronie, mogą być udostępniane wyłącznie osobie upoważnionej i tylko w zakresie niezbędnym do wykonywania obowiązków na zajmowanym stanowisku lub realizacji umów lub zadań służbowych.
- przechowywanie informacji podlegających „ochronie" powinno zabezpieczać je przed wglądem osób nieuprawnionych.
- wykonawca dokumentu „chronionego" i osoba, której go przekazano, odpowiadają za właściwe jego zabezpieczenie przed dostępem osób nieuprawnionych, zagubieniem, zniszczeniem lub kradzieżą.
- Wysyłając pismo lub faks należy sprawdzić dokładnie adres odbiorcy. Konsekwencje wysłania do niewłaściwego odbiorcy mogą być istotne.
- Informacje podlegające „ochronie", należy wykonać wyłącznie w niezbędnej, maksymalnie ograniczonej ilości kopii.
- W czasie wystąpień publicznych, chcąc się wykazać kompetencją, nie należy przekazywać nieznanych powszechnie informacji o wynikach badań, metodach

rozwiązywania problemów, środkach bezpieczeństwa, itp. Nie staraj się udowadniać w kontaktach zewnętrznych, że jesteś ważny, mówiąc więcej niż powinieneś.

- Rozmowy przez telefon:
  - żaden telefon nie może być traktowany jako bezpieczny i dlatego należy unikać przekazywania w ten sposób informacji podlegających „ochronie”,
  - przed przekazaniem informacji należy upewnić się, że rozmowa nie będzie słyszana przez osoby postronne. Należy unikać rozmów w miejscach publicznych,
  - jeżeli nie rozpoznajesz jednoznacznie głosu osoby, z którą rozmawiasz, potwierdź jej tożsamość. W razie wątpliwości, przerwij rozmowę i oddzwoń.
- Wiarygodność i ochrona dokumentów:
  - istotne dokumenty należy podpisywać pełnym imieniem i nazwiskiem. Przed podpisaniem jakiegokolwiek dokumentu służbowego, zastanów się czy masz uprawnienia do tej czynności i jakie mogą wyniknąć z tego konsekwencje;
  - dokumenty drukowane na drukarkach znajdujących się w miejscach ogólnie dostępnych (korytarze, sekretariaty, itp.), należy zabierać natychmiast po wydrukowaniu;
  - wykorzystanie z nośników przenośnych jest dopuszczalne tylko przy użyciu szyfrowania sprzętowego lub programowego przenoszonej zawartości;
  - po wykorzystaniu, nośniki informacji podlegających „ochronie” należy zniszczyć w sposób trwały i uniemożliwiający odczytanie ich treści. Dokumenty papierowe, płytki CD/DVD w odpowiedniej niszczarce lub z wykorzystaniem bezpiecznego pojemnika. Nie wyrzucaj do śmieci, bez trwałego zniszczenia, dokumentów, które nie są publicznie znane.

Bezpieczeństwo informatyczne

- Decyzje o założeniu konta dla użytkownika, podłączeniu urządzeń (serwerów, stacji roboczych, drukarek, skanerów, elementów infrastruktury sieciowej LAN i WAN, urządzeń specjalnych itp.) do systemu informatycznego wydaje Administrator Danych Osobowych. Założenie kont i podłączenie urządzeń odbywa się z wykorzystaniem wniosku.

- Dział IT ma prawo do monitorowania pracy użytkowników w Systemie. Administrator Danych Osobowych lub osoby przez niego upoważnione mają prawo wglądu do wszystkich zasobów użytkownika w Systemie.
- Użytkownicy systemu informatycznego mają obowiązek:
  - dbać o stan i właściwe użytkowanie urządzeń im powierzonych, w tym zapobiegać kradzieży i nieupoważnionemu użytkowaniu własnej stacji roboczej;
  - archiwizować na bieżąco dane ze swojej stacji roboczej;
  - wykorzystywać zaimplementowane służbowo zabezpieczenia techniczne w celu ochrony poufności, dostępności i integralności wytwarzanych, przetwarzanych i przechowywanych danych;
  - utrzymania w sekrecie danych uwierzytelniających umożliwiających dostęp do urządzeń i systemów;
  - zabezpieczyć dane uwierzytelniające do kont, poprzez stosowanie odpowiednich haseł i praw dostępu do swoich zasobów. Należy stosować minimalną długość hasła na 12 znaków, zawierające dużą i małą literę oraz znak specjalny. Hasła należy zmieniać nie rzadziej niż raz w roku;
  - natychmiastowej zmiany hasła w przypadku podejrzenia jego kompromitacji (przejęcie lub upublicznienie hasła);
  - wszystkie dane uwierzytelniające domyślne otrzymane od producentów sprzętu i oprogramowania, Działu IT lub kontrahenta powinny być natychmiast zmienione;
  - bezwzględnie stosować się do uwag i zaleceń pracowników Działu IT w zakresie bezpiecznego użytkowania Systemu;
  - przestrzegać poufności innych kont w systemie i nie ingerować w ich zasoby, nawet jeśli nie są one stosownie „chronione”;
  - umożliwiać dostęp do powierzonych zasobów w systemie tylko osobom uprawnionym;
  - niezwłocznie informować o wszelkich incydentach naruszenia bezpieczeństwa informatycznego oraz cyberbezpieczeństwa i udzielać niezbędnych wyjaśnień.
- Użytkownikowi systemu informatycznego nie wolno:

- ustanawiać haseł zawierających przewidywalne człony np. szpitala, kontrahenta, nazwa usługi, nazwa systemu, imię, nazwisko, datę urodzenia itp.;
- zabrania się zapisywania danych uwierzytelniających (na kartkach, w plikach tekstowych, w przeglądarkach itp.);
- korzystać z usług, oprogramowania i aplikacji oraz instalacji nie dopuszczonych do użytkowania w PCZ przez Administratora Danych Osobowych;
- udostępniać swojego konta (w tym danych uwierzytelniających) innym osobom;
- wykorzystywać system w celach niedozwolonych prawem polskim i międzynarodowym oraz regulacjami wewnętrznymi PCZ;
- działać na szkodę innych użytkowników systemu lub podejmować działania wskazujące na takie zamiary;
- udzielać osobom nieuprawnionym jakichkolwiek informacji dotyczących systemu informatycznego;
- podejmować jakichkolwiek działań mogących spowodować utratę stabilności systemu informatycznego;
- podłączać samodzielnie do zasobów PCZ urządzeń nie autoryzowanych przez Dział IT;
- tworzenia repozytorium plików w darmowych usługach udostępniających przestrzeń dyskową (np. Dropbox, Dysk google);
- ustawiać bezpośrednich forwardów na skrzynki pocztowe na zewnątrz (u klienta, na darmowym serwerze, itp.);
- na serwerach w internecie używać haseł identycznych z hasłami, których używasz w systemie. Nie słuchaj apeli o dostosowaniu konfiguracji Twojego oprogramowania klienckiego lub samodzielnej instalacji dodatkowych modułów (np. plug-in);

– <u>zasady wymiany i udostępniania plików zwierających informacje chronione:</u>
  - wszystkie pliki powinny być zabezpieczone przed nieuprawnionym dostępem;
  - akceptowane sposoby bezpiecznej wymiany plików:
    - zabezpieczenie plików hasłem w aplikacji (np. Excel, Word, PowerPoint);
    - spakowanie plików narzędziem 7zip i zabezpieczenie archiwum hasłem.

– <u>zasady bezpiecznej komunikacji</u>:

- rekomendowane narzędziem jest MS Teams;
- potwierdzenie wszystkich uczestników spotkania;
- wyświetlanie tylko materiałów przeznaczonych dla uczestników spotkania poprzez prezentację wskazanego okna;
- nieudostępnianie pulpitu jako okna, ze względu na brak kontroli nad komunikatami i wiadomościami.

– Dział IT ma prawo ograniczyć Twój dostęp do zasobów internetu. Jeżeli Twoje obowiązki wymagają sięgania do zablokowanych serwisów, zgłoś oficjalnie prośbę o zmianę uprawnień.
– Pamiętaj, że w przypadku, kiedy logi wskazują na umyślne łamanie zasad dotyczących bezpieczeństwa połączeń z internetem, mogą być stosowane restrykcje służbowe.
– Nie otwieraj e-maili od nieznanych lub niesprawdzonych adresatów, nie odpowiadaj na oferty przesyłane jako reklamówki lub spam.

Kontrola ruchu osobowego w obiektach

– Prawo wejścia do stref chronionych PCZ mają osoby, którym wydano właściwe uprawnienia dostępu do pomieszczeń. O uprawnieniach decydują osoby, które zarządzają danymi pomieszczeniami.
– Dokumentami uprawniającymi do wejścia i przebywania na terenie obiektu są również legitymacje służbowe wraz z pisemnym upoważnieniem imiennym, będące w posiadaniu urzędników i funkcjonariuszy, których uprawnienia normują odrębne przepisy. Upoważnień takich nie muszą posiadać osoby działające w ramach akcji ratowniczej.
– Wszyscy pracownicy zobowiązani są chronić karty zbliżeniowe (SKD) i klucze fizyczne, celem niedopuszczenia do ich utraty lub zniszczenia. Zabrania się również udostępniania ich osobom trzecim.
– W przypadku utraty karty zbliżeniowej/klucza należy niezwłocznie zgłosić incydent bezpieczeństwa informacji.
– Nie pozostawiaj w pomieszczeniach PCZ, bez opieki, gościa lub interesanta. Jesteś za niego odpowiedzialny i masz obowiązek towarzyszyć mu przez cały czas.
–

– Nigdy nie zostawiaj bez nadzoru kluczy w miejscu, w którym osoba nieuprawniona może mieć do nich dostęp (np. na zewnątrz drzwi do pokoju, na półce, parapecie, haczyku na ścianie). Ustal zasady przekazywania kluczy z pozostałymi osobami, które z nich korzystają.

Delegacje krajowe i zagraniczne

– Nie pozostawiaj sprzętu i zapisanych nośników danych bez nadzoru lub w miejscu o niewystarczającej ochronie (np. na siedzeniu samochodu, w bagażniku).
– Nie rozmawiaj o sprawach służbowych z przypadkowymi osobami i w przypadkowych miejscach. Jeżeli rozmawiasz o istotnych sprawach służbowych, zachowaj szczególną ostrożność w odniesieniu do rozmówcy i miejsca (nie rób tego w pociągu czy w samolocie).
– Hotel nie jest w pełni bezpiecznym miejscem pracy oraz rozmów i spotkań.

Incydenty Bezpieczeństwa Informacji

– Obowiązkiem każdego pracownika jest niezwłoczne przekazywanie informacji o podejrzeniu wystąpienia lub wystąpieniu incydentu bezpieczeństwa informacji (w tym w odniesieniu do cyberbezpieczeństwa i danych osobowych) poprzez wysłanie maila na adres incydent@pczkartuzy.pl (pracownik lub współpracownik, który nie posiada dostępu do poczty elektronicznej wykonuje zgłoszenie do bezpośredniego przełożonego lub Pełnomocnika ds. Cyberbezpieczeństwa) w czasie nieprzekraczającym 4 godzin od powzięcia informacji o wystąpieniu incydentu.
– W ramach prowadzonego postępowania wyjaśniającego, pracownicy zobowiązani są do udzielania wyjaśnień i przekazywania informacji na każde żądanie osoby wyznaczonej do obsługi incydentu bezpieczeństwa.

Zasady współpracy z Policją, jednostkami Straży Pożarnej i Straży Miejskiej

– Współpraca i współdziałanie oraz wymiana Informacji o zagrożeniach w zakresie bezpieczeństwa osób i mienia oraz zakłócenia spokoju publicznego oraz następuje poprzez:
  - współdziałaniu przy zabezpieczeniu miejsc popełnienia przestępstw i wykroczeń w granicy chronionych obiektów,
  - zabezpieczenie śladów na miejscu zdarzenia,

- niedopuszczenie osób postronnych na miejscu zdarzenia,
- współdziałanie w zabezpieczeniu powstałych awarii na terenie spółki,
- udzielenie wzajemnej pomocy przy realizacji zadań ochrony i zapobieganiu przestępczości,
- udzielanie wyczerpujących informacji o zagrożeniach dla bezpieczeństwa i porządku publicznego,
- pomoc w ustaleniu świadków zdarzenia,
- wykonywanie innych czynności zleconych przez Policję.

– O zaistniałej awarii, pożarze, Pracownik lub inna osoba, zawiadamia Straż Pożarną oraz Prezesa Zarządu. Przybyłe jednostki ratownicze należy niezwłocznie skierować na miejsce zdarzenia. Szczegółowe postanowienia na temat podejmowanych w tym zakresie działań zostały opisane w dokumentacji systemu zarządzania, w tym w Instrukcjach Bezpieczeństwa Pożarowego.

ZATWIERDZIŁ

Prezes Zarządu Paweł Witkowski