Projekt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
Szpital

1. Identyfikacja kluczowych aktywów informacyjnych

1.1. Dane osobowe pacjentów, lekarzy, służby medycznej

- **Zawartość:** Imiona, nazwiska, numery PESEL, adresy zamieszkania, dane kontaktowe, stanowiska**.**
- **Znaczenie prawne:** Dane są chronione przez RODO oraz krajowe regulacje dotyczące ochrony danych osobowych.
- **Znaczenie dla ciągłości działania:** Kluczowe dla organizacji pracy personelu, komunikacji z pacjentami oraz zarządzania ich opieką zdrowotną.

1.2. Systemy zarządzania personelem

- **Zawartość:** Grafiki dyżurów, listy obecności, szczegóły umów o pracę.
- **Znaczenie prawne:** Przestrzeganie przepisów dotyczących czasu pracy, umów o pracę oraz ochrony danych pracowników.
- **Znaczenie dla ciągłości działania:** Fundamentalne dla organizacji pracy, pomaga w unikaniu konfliktów grafików i zapewnia optymalne pokrycie zmian w celu ciągłości opieki nad pacjentami.

1.3. Historia leczenia pacjentów

- **Zawartość:** Dokumentacja medyczna zawierająca historię diagnoz, przeprowadzonych zabiegów, wydanych recept, zaleceń lekarskich.
- **Znaczenie prawne:** Dokumentacja medyczna musi być przechowywana zgodnie z przepisami prawa o archiwizacji danych medycznych.
- **Znaczenie dla ciągłości działania:** Niezbędna do zapewnienia prawidłowego leczenia i opieki nad pacjentami, szczególnie w przypadku przekazywania pacjenta między specjalistami lub przy ponownych wizytach.

1.4. Dane i systemy finansowe

- **Zawartość:** Faktury, wynagrodzenia, rozliczenia z NFZ, konta bankowe, konta bankowe i systemy płatności, rozliczenia z dostawcami i kontrahentami
- **Znaczenie prawne:** Muszą być przetwarzane i przechowywane zgodnie z prawem podatkowym, rachunkowym oraz regulacjami finansowymi.

- **Znaczenie dla ciągłości działania:** Zapewniają zdolność instytucji do zarządzania budżetem, regulowania zobowiązań i uzyskiwania środków na działalność.

1.5. Dane infrastrukturalne i logistyczne

- **Zawartość:** Harmonogramy dostaw i logistyki (dostawy leków, sprzętu, artykułów sanitarnych), systemy zarządzania sprzętem medycznym, systemy zarządzania lekami (np. magazyn leków)
- **Znaczenie prawne:** Przepisy MDR (Medical Device Regulation), kontrola techniczna sprzętu
- **Znaczenie dla ciągłości działania:** Są kluczowe dla ciągłości leczenia i unikania opóźnień zagrażających życiu pacjentów.

2. Analiza ryzyk:

Zagrożenie	Konsekwencje i koszty naruszenia	Częstość występowania	Wpływ na ciągłość działania firmy
Atak hakerski (ransomware, phishing)	Utrata dostępu do EDM, wyciek danych pacjentów, szantaż	Średnia	Krytyczny
Nieautoryzowany dostęp do systemu szpitalnego	Naruszenie RODO, kary finansowe	Średnia	Wysoki
Awaria systemów IT	Opóźnienia w działaniu szpitala, brak dostępu do danych	Niska	Krytyczny
Awaria prądu	Przestoje w działaniu sprzętu medycznego, opóźnienia w leczeniu, koszty odzyskania funkcjonalności	Niska	Krytyczny
Złośliwe oprogramowanie (wirusy, trojany)	Przejęcie wrażliwych danych, uszkodzenie systemu	Wysoka	Wysoki
Błąd pracownika (np. wysłanie danych pacjenta na zły adres e-mail)	Naruszenie RODO, potencjalne kary finansowe, naruszenie prywatności pacjentów	Średnia	Średni

Kradzież sprzętu (np. laptopów, pendrive'ów)	Możliwy wyciek danych, koszt zakupu nowego sprzętu	Średnia	Wysoki
Kradzież dokumentacji papierowej	Utrata poufnych informacji	Niska	Średni
Problemy prawne	Naruszenie praw autorskich, brak odpowiednich licencji	Niska	Wysoki
Pożar, powódź lub inne zdarzenia losowe	Całkowita utrata danych fizycznych, koszt odbudowy systemów	Niska	Krytyczny
Brak przeszkolenia personelu	Zwiększona podatność na ataki socjotechniczne, błędy proceduralne	Wysoka	Niski
Problemy z aktualizacją oprogramowania	Luka w zabezpieczeniach, zwiększone ryzyko ataku cybernetycznego	Niska	Średni

Odniesienie do norm:

- **Atak hakerski (ransomware, phishing)**
  - **ISO/IEC 27002, pkt 5.26** ***"Response to information security incidents"*** - zawiera informacje o odpowiedzi na incydenty bezpieczeństwa informacji, co ma znaczenie w kontekście ataków hakerskich, gdzie szybka i skuteczna reakcja jest kluczowa.
  - **ISO/IEC 27002, pkt 5.7** ***"Threat intelligence"*** **–** skupia się na zbieraniu, analizowaniu i wykorzystywaniu informacji o zagrożeniach, aby zwiększyć świadomość organizacji na temat potencjalnych ryzyk i skutecznie je mitigować.
- **Nieautoryzowany dostęp do systemu szpitalnego**
  - **ISO/IEC 27002, pkt 7.1** ***"Physical security perimeters"*** **–** zabezpieczenia przeciw włamaniu

- **ISO/IEC 27002, pkt 7.2** ***"Physical entry"*** **–** system kontroli dostępu (karty, klucze, rejestrowanie wejść).
- **ISO/IEC 27002, pkt 5.15** ***"Access control"*** **–** uwzględnienie zasad ograniczenia dostępu i uprawnień

- **Awaria systemów informatycznych**
  - **ISO/IEC 27002, pkt 5.30** ***"ICT readiness for business continuity"*** **–** zapewnienie ciągłości działania systemów IT, w tym plany awaryjne i procedury odzyskiwania.
  - **ISO/IEC 27002, pkt 8.14** ***"Redundancy of information processing facilities"*** **–** strategie redundancji, regularne testowanie kopii zapasowych i procedur odtwarzania systemów.
- **Awaria prądu:**
  - **ISO/IEC 27002, pkt 5.30** ***"ICT readiness for business continuity"*** **–** wymaga przygotowania systemów (np. zapasowy generator prądu) tak, aby krytyczne usługi takie jak trwające operacje lub pacjenci wymagający sprzętu medycznego mogły działać także w razie braku zasilania
- **Złośliwe oprogramowanie (wirusy, trojany)**
  - **ISO/IEC 27002, pkt 8.7** ***"Protection against malware"*** - wskazuje m.in. na potrzebę implementacji skutecznych narzędzi antymalware, w tym oprogramowania antywirusowego, systemów prewencyjnych, regularnych aktualizacji definicji wirusów oraz skanów bezpieczeństwa.
- **Błąd pracownika (np. wysłanie danych pacjenta na zły adres e-mail)**
  - **ISO/IEC 27002, pkt 5.14** ***"Information transfer"*** - zawiera zasady bezpiecznego przekazywania informacji, które mogą obejmować metody zapewnienia, że dane są wysyłane do odpowiednich osób i przez odpowiednie kanały.
- **Kradzież danych**
  - **ISO/IEC 27002, pkt 7,10** ***"Storage media"*** - wykonywanie wielu kopii dokumentów na nośnikach, odpowiednie czyszczenie nośników przed ponownym użyciem.
- **Brak przeszkolenia personelu**
  - **ISO/IEC 27002, pkt 6.3** ***"Information security awareness, education and training"*** **–** obowiązkowe szkolenia z zakresu ochrony danych medycznych, cyberbezpieczeństwa i procedur reagowania na incydenty.

- **ISO/IEC 27002, pkt 5.4 *"Management responsibilities"* –** odpowiedzialność kierownictwa za wdrażanie programów edukacyjnych i podnoszenie świadomości pracowników.
- **ISO/IEC 27002, pkt 6.4 *"Disciplinary process"* –** określenie konsekwencji nieprzestrzegania zasad bezpieczeństwa, np. udostępniania haseł lub obchodzenia systemów zabezpieczeń.

- **Pożar, powódź lub inne zdarzenia losowe**
  - **ISO/IEC 27002, pkt 5.29 *"Information security during disruption"* –** pomaga zapewnić ciągłość ochrony informacji w trudnych warunkach.

3. Propozycja polityki bezpieczeństwa:

Ochrona fizyczna

- **Patrolowanie obszarów krytycznych (serwerownia, magazyn leków, archiwum dokumentacji pacjentów)**
  - **ISO/IEC 27002, pkt 7.4 *"Physical security monitoring"*** – systemy CCTV, kontrola dostępu, monitoring obszarów wrażliwych.
- **Kontrola dostępu do budynku i stref o ograniczonym dostępie (np. oddział intensywnej terapii, sale operacyjne, laboratoria)**
  - **ISO/IEC 27002, pkt 7.2 *"Physical entry"*** – system kart dostępu, rejestrowanie wejść i wyjść.

Recepcja / Rejestracja pacjentów

- **Weryfikacja tożsamości pacjentów przed udzieleniem świadczeń medycznych**
  - **ISO/IEC 27002, pkt 5.16 *"Identity management"*** – procedury potwierdzania tożsamości pacjenta, np. poprzez dokumenty lub dane biometryczne.
- **Ochrona wrażliwych danych pacjentów w systemie rejestracji**
  - **ISO/IEC 27002, pkt 5.15 *"Access control"*** – ograniczenie dostępu do informacji zdrowotnych wyłącznie dla upoważnionych osób.

Personel medyczny

- **Dostęp do elektronicznej dokumentacji medycznej (EDM) zgodnie z zakresem obowiązków**
  - **ISO/IEC 27002, pkt 5.18 *"Access rights"*** – nadawanie i ograniczanie uprawnień do EDM.
- **Zabezpieczenie stanowisk pracy przed nieautoryzowanym dostępem (np. blokowanie ekranu, czysta karta pracy)**

- **ISO/IEC 27002, pkt 7.7** ***"Clear desk and clear screen"*** – ochrona poufnych danych przed dostępem osób trzecich**.**

Dział IT / Administrator systemu

- **Zarządzanie uprawnieniami użytkowników – przydzielanie, modyfikowanie i odbieranie dostępu**
  - **ISO/IEC 27002, pkt 5.18** ***"Access rights"*** – ścisła kontrola dostępu do systemów szpitalnych.
- **Regularne aktualizacje systemów medycznych i infrastruktury IT**
  - **ISO/IEC 27002, pkt 8.8** ***"Management of technical vulnerabilities"*** – eliminacja podatności, stosowanie poprawek zabezpieczeń.
- **Tworzenie i testowanie kopii zapasowych systemów szpitalnych**
  - **ISO/IEC 27002, pkt 8.13** ***"Information backup"*** – zapewnienie ciągłości działania w przypadku awarii.

Apteka szpitalna / Magazyn leków

- **Kontrola dostępu do leków i substancji kontrolowanych**
  - **ISO/IEC 27002, pkt 7.1** ***"Physical security perimeters"*** – fizyczne zabezpieczenie magazynów leków.
- **Zarządzanie danymi o zapasach leków i ich dystrybucji**
  - **ISO/IEC 27002, pkt 5.12** ***"Classification of information"*** – odpowiednia klasyfikacja i ochrona danych o lekach.

Kierownictwo szpitala

- **Akceptacja ryzyka związanego z cyberbezpieczeństwem i zarządzaniem danymi medycznymi**
  - **ISO/IEC 27002, pkt 5.4** ***"Management responsibilities"*** – określenie poziomu ryzyka akceptowalnego dla organizacji.
- **Planowanie ciągłości działania w przypadku awarii systemów IT lub zagrożeń fizycznych**
  - **ISO/IEC 27002, pkt 5.30** ***"ICT readiness for business continuity"*** – przygotowanie strategii na wypadek incydentów informatycznych.
- **Informowanie wszystkich pracowników o wprowadzanych zasadach bezpieczeństwa**
  - **ISO/IEC 27002, pkt 6.3** ***"Information security awareness, education and training"***

Dział Komunikacji i Dokumentacji Medycznej

- **Zarządzanie przepływem dokumentacji pacjentów i ochrona ich prywatności**
    - **ISO/IEC 27002, pkt 5.34** ***"Privacy and protection of PII"*** – przetwarzanie danych zgodnie z przepisami o ochronie prywatności (np. RODO).
- **Bezpieczna archiwizacja i niszczenie dokumentacji medycznej**
    - **ISO/IEC 27002, pkt 5.33** ***"Protection of records"*** – określenie zasad przechowywania i utylizacji danych medycznych.

4. Procesy i dokumentacja procesowa

Postępowanie w razie naruszenia polityki bezpieczeństwa informacji

- **Wykrycie naruszenia polityki** – Jeśli naruszenie polityki bezpieczeństwa zostanie wykryte przez systemy monitorujące lub pracownika, należy natychmiast zgłosić incydent do zespołu ds. bezpieczeństwa.
    - **ISO/IEC 27002, 5.1** ***"Policies for information security"*** – Tworzenie i wdrażanie polityk bezpieczeństwa informacji w organizacji.
- **Ocena skutków naruszenia** – Zespół ds. bezpieczeństwa powinien przeanalizować, jakie dane lub systemy zostały dotknięte naruszeniem, oraz ocenić potencjalny wpływ na organizację.
    - **ISO/IEC 27002, 5.25** ***"Assessment and decision on information security events"*** – Ocena incydentów związanych z bezpieczeństwem informacji.
- **Reakcja i naprawa** – Należy podjąć działania mające na celu naprawienie naruszenia, takie jak zmiana haseł, dostosowanie konfiguracji systemów czy wprowadzenie nowych mechanizmów kontroli.
    - **ISO/IEC 27002, 5.26** ***"Response to information security incidents"*** – Procedury reagowania na incydenty związane z bezpieczeństwem informacji.
- **Przeprowadzenie audytu** – Po usunięciu skutków naruszenia, organizacja powinna przeprowadzić audyt w celu sprawdzenia, czy incydent nie powtarza się w przyszłości.
    - **ISO/IEC 27002, 5.35** ***"Independent review of information security"*** – Niezależne przeglądy bezpieczeństwa informacji.

Postępowanie w razie utraty integralności danych

- **Wykrycie utraty integralności** – System monitorowania powinien natychmiast zgłosić wykrycie utraty integralności danych, takie jak zmiany w plikach lub bazach danych bez autoryzacji.

    - **ISO/IEC 27002, 8.5** ***"Access to source code"*** **–** Zapewnienie kontroli dostępu do kodu źródłowego w celu ochrony przed nieautoryzowanymi zmianami.

- **Analiza incydentu** – Zespół ds. bezpieczeństwa i zarządzania danymi powinien zidentyfikować zakres utraty integralności, ustalić, które dane zostały zmodyfikowane, oraz przeprowadzić analizę, czy dane zostały zmienione celowo.

    - **ISO/IEC 27002, 5.7** ***"New Threat intelligence"*** **–** Zbieranie informacji o zagrożeniach i analizowanie ich w kontekście utraty integralności danych.

- **Przywrócenie danych** – Dane powinny zostać przywrócone z kopii zapasowych, aby zapewnić ich integralność i dostępność.

    - **ISO/IEC 27002, 8.13** ***"Information backup"*** **–** Zapewnienie kopii zapasowych danych w celu ich przywrócenia.

- **Zapobieganie powtórzeniu się incydentu** – Organizacja powinna wprowadzić dodatkowe kontrole, aby zapobiec podobnym incydentom w przyszłości, takie jak szyfrowanie danych czy zmiana polityki dostępu.

    - **ISO/IEC 27002, 8.4** ***"Information access restriction"*** **–** Ograniczenie dostępu do wrażliwych informacji w celu ochrony integralności.

Postępowanie w razie utraty dostępności systemu (awaria systemu)

- **Wykrycie awarii** – Jeśli system wykryje awarię lub przestanie działać, powinien automatycznie poinformować odpowiedni zespół ds. wsparcia technicznego.

    - **ISO/IEC 27002, 5.29** ***"Information security during disruption"*** **–** Planowanie utrzymania bezpieczeństwa informacji podczas zakłóceń, takich jak awarie systemów.

- **Analiza awarii** – Zespół odpowiedzialny za ciągłość działania powinien określić przyczynę awarii i oszacować czas, jaki będzie potrzebny do przywrócenia systemu do pełnej funkcjonalności.

    - **ISO/IEC 27002, 8.14** ***"Redundancy of information processing facilities"*** **–** Zapewnienie redundancji w celu minimalizacji skutków awarii systemów.

- **Przywrócenie systemów** – W razie awarii, należy jak najszybciej uruchomić zapasowe systemy lub usługi, a także przywrócić dane z kopii zapasowych, aby przywrócić pełną dostępność.

    - **ISO/IEC 27002, 8.13** ***"Information backup"*** **–** Przywracanie danych z kopii zapasowych w przypadku awarii.

- **Testowanie i ocena** – Po usunięciu awarii, należy przetestować systemy, aby upewnić się, że działa on prawidłowo i jest zabezpieczony przed przyszłymi awariami.

    - **ISO/IEC 27002, 8.16** ***"Monitoring activities"*** **–** Monitorowanie działalności systemów w celu zapewnienia ich stabilności po awarii.

Postępowanie w razie ataku DDoS (Distributed Denial of Service)

- Wykrycie ataku DDoS – Systemy monitorujące ruch sieciowy powinny wykryć nadmiarowe zapytania do serwerów i natychmiast powiadomić administratorów.
    - **ISO/IEC 27002, 13.1.1** ***"Network security"*** **–** Zabezpieczenie sieci przed atakami, takimi jak DDoS.
- Zmniejszenie skutków ataku – Należy wdrożyć mechanizmy przeciwdziałania DDoS, takie jak zwiększenie przepustowości serwerów lub użycie zapór sieciowych do zablokowania atakujących adresów.
    - **ISO/IEC 27002, 8.7** ***"Protection against malware"*** **–** Zabezpieczenie przed złośliwym oprogramowaniem, w tym atakami DDoS.
- Analiza i raportowanie – Po zakończeniu ataku należy przeanalizować jego źródło oraz wpływ na organizację, przygotować raport o przebiegu ataku i wdrożyć środki zapobiegawcze.
    - **ISO/IEC 27002, 5.24** ***"Information security incident management planning and preparation"*** **–** Planowanie i przygotowanie na incydenty związane z bezpieczeństwem informacji.
- Wdrażanie działań zapobiegawczych – Organizacja powinna wdrożyć dodatkowe mechanizmy ochrony przed przyszłymi atakami DDoS, takie jak filtrowanie ruchu czy wykorzystywanie zewnętrznych usług ochrony przed DDoS.
    - **ISO/IEC 27002, 5.29** ***"Information security during disruption"*** **–** Planowanie utrzymania bezpieczeństwa w czasie zakłóceń, w tym ataków DDoS.

Postępowanie w razie naruszenia prywatności danych osobowych

- Wykrycie naruszenia prywatności – Jeśli dojdzie do wycieku lub nieautoryzowanego ujawnienia danych osobowych, organizacja powinna natychmiast uruchomić procedury reakcji na incydent.
    - **ISO/IEC 27002, 5.34** ***"Privacy and protection of PII"*** **–** Ochrona prywatności i danych osobowych (PII).
- Powiadomienie odpowiednich organów – Po wykryciu naruszenia prywatności, organizacja powinna natychmiast powiadomić odpowiednie organy nadzoru zgodnie z wymaganiami prawnymi.
    - **ISO/IEC 27002, 5.34** ***"Privacy and protection of PII"*** **–** Zgodność z wymaganiami ochrony danych osobowych.
- Ocena wpływu naruszenia – Zespół ochrony danych osobowych powinien przeprowadzić dokładną ocenę skutków naruszenia i podjąć działania naprawcze, w tym powiadomienie osób, których dane zostały ujawnione.

    - **ISO/IEC 27002, 18.1.4** ***“Privacy and protection of PII”*** **–** Ochrona danych osobowych i prywatności.

- Wdrażanie środków zaradczych – Organizacja powinna zidentyfikować luki, które pozwoliły na naruszenie prywatności, i wprowadzić odpowiednie środki zaradcze.
    - **ISO/IEC 27002, 5.5** ***“Contact with authorities”*** **–** Kontakt z odpowiednimi władzami i organami nadzorczymi w przypadku naruszenia prywatności danych.