Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
A.5	**Zabezpieczenia organizacyjne**			
A.5.1	Polityki bezpieczeństwa informacji	Polityka bezpieczeństwa informacji i polityki tematyczne powinny być określone, zatwierdzone przez kierownictwo, zakomunikowane właściwemu personelowi i właściwym stronom zainteresowanym, uznane przez nich oraz poddawane przeglądom w zaplanowanych odstępach czasu i jeżeli wystąpią istotne zmiany.	Tak, zabezpieczenie wdrożono. Polityka bezpieczeństwa informacji i polityki tematyczne Szpital są określone, zatwierdzone przez Dyrekcję Szpitala, zakomunikowane właściwemu personelowi i właściwym stronom zainteresowanym, uznane przez Szpital oraz poddawane przeglądom w zaplanowanych odstępach czasu i jeżeli wystąpią istotne zmiany. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji.	Nie dotyczy
A.5.2	Role i odpowiedzialność za bezpieczeństwo informacji	Role i odpowiedzialność za bezpieczeństwo informacji powinny być określone i przypisane zgodnie z potrzebami organizacji.	Tak, zabezpieczenie wdrożono. Role i odpowiedzialność za bezpieczeństwo informacji Szpitala są określone i przypisane zgodnie z potrzebami organizacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	Nie dotyczy
A.5.3	Rozdzielanie obowiązków	Obowiązki i obszary odpowiedzialności pozostające ze sobą w konflikcie należy rozdzielić.	Tak, zabezpieczenie wdrożono. Obowiązki i obszary odpowiedzialności pozostające ze sobą w konflikcie zostały rozdzielone.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-11-U - Procedura użytkowania sieci telein-formatycznej;	
A.5.4	Odpowiedzialność kierownictwa	Kierownictwo powinno wymagać, aby cały personel stosował zasady bezpieczeństwa informacji zgodnie z ustanowionymi w organizacji polityką bezpieczeństwa, politykami tematycznymi i procedurami.	Tak, zabezpieczenie wdrożono. Dyrekcja Szpitala wymaga, aby cały personel stosował zasady bezpieczeństwa informacji zgodnie z ustanowionymi w organizacji polityką bezpieczeństwa, politykami tematycznymi i procedurami. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-04-U - Procedura nadawania upoważnień; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	Nie dotyczy
A.5.5	Kontakty z organami władzy	Organizacja powinna ustanowić i utrzymywać kontakty z właściwymi organami władzy.	Tak, zabezpieczenie wdrożono. Szpital ustanowiła i utrzymuje kontakty z właściwymi organami władzy. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji.	Nie dotyczy
A.5.6	Kontakty z grupami zainteresowanych specjalistów	Organizacja powinna ustanowić i utrzymywać kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi	Tak, zabezpieczenie wdrożono. Szpital ustanowił i utrzymuje kontakty z grupami zainteresowanych specjalistów lub innymi	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
		forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa.	specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji.	
A.5.7	Rozpoznanie zagrożeń	Informacje dotyczące zagrożeń dla bezpieczeństwa informacji powinny być zbierane i analizowane w celu ich rozpoznania.	Tak, zabezpieczenie wdrożono. Informacje dotyczące zagrożeń dla bezpieczeństwa informacji w Szpital są zbierane i analizowane w celu ich rozpoznania. Dokument tematyczny stanowi: SZBI-07-U - Procedura oceny skutków; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-19-U - Procedura privacy by design, privacy by default;	Nie dotyczy
A.5.8	Bezpieczeństwo informacji w zarządzaniu projektami	Bezpieczeństwo informacji powinno być zintegrowane z zarządzaniem projektami.	Tak, zabezpieczenie wdrożono. Bezpieczeństwo informacji w Szpital jest zintegrowane z zarządzaniem projektami. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-07-U - Procedura oceny skutków; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-18-U - Procedura zarządzania zmianą IT;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-19-U - Procedura privacy by design, privacy by default.	
A.5.9	Ewidencja informacji i innych powiązanych aktywów	Należy opracować i utrzymywać ewidencję informacji i innych powiązanych aktywów, w tym ich właścicieli.	Tak, zabezpieczenie wdrożono. Szpital opracował i utrzymuje ewidencję informacji i innych powiązanych aktywów, w tym ich właścicieli. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi;	Nie dotyczy
A.5.10	Akceptowalne użycie informacji i innych powiązanych aktywów	Należy zidentyfikować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji i innych powiązanych aktywów oraz procedury postępowania z informacjami i innymi powiązanymi aktywami.	Tak, zabezpieczenie wdrożono. Szpital zidentyfikowano, udokumentowano i wdrożono zasady akceptowalnego użycia informacji i innych powiązanych aktywów oraz procedury postępowania z informacjami i innymi powiązanymi aktywami. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi.	Nie dotyczy
A.5.11	Zwrot aktywów	Personel i inne strony zainteresowane, jeśli jest to właściwe, powinny zwrócić wszystkie posiadane aktywa organizacji w momencie zmiany lub zakończenia zatrudnienia, umowy lub porozumienia.	Tak, zabezpieczenie wdrożono. Personel Szpital i inne strony zainteresowane, jeśli jest to właściwe, zwracają wszystkie posiadane aktywa organizacji w momencie zmiany lub zakończenia zatrudnienia, umowy lub porozumienia.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			Dokument tematyczny stanowi: SZBI-20-U - Procedura zarządzania aktywami informacyjnymi; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich; SZBI-30-P - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców.	
A.5.12	Klasyfikowanie informacji	Informacje powinny być klasyfikowane zgodnie z potrzebami organizacji w zakresie bezpieczeństwa informacji na podstawie poufności, integralności, dostępności oraz wymagań właściwych stron zainteresowanych.	Tak, zabezpieczenie wdrożono. Informacje Szpital są klasyfikowane zgodnie z potrzebami Szpital w zakresie bezpieczeństwa informacji na podstawie poufności, integralności, dostępności oraz wymagań właściwych stron zainteresowanych. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników; SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
A.5.13	Oznaczanie informacji	Należy opracować i wdrożyć odpowiedni zbiór procedur oznaczania informacji zgodnie z przyjętym w organizacji schematem klasyfikacji informacji.	W Szpital opracowano i wdrożono odpowiedni zbiór procedur oznaczania informacji zgodnie z przyjętym w organizacji schematem klasyfikacji informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi; SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.	Nie dotyczy
A.5.14	Przesyłanie informacji	Należy wdrożyć zasady, procedury lub umowy dotyczące przesyłania informacji dla wszystkich typów środków przekazywania w ramach organizacji oraz między organizacją a innymi stronami.	Tak, zabezpieczenie wdrożono. W Szpital wdrożono zasady, procedury lub umowy dotyczące przesyłania informacji dla wszystkich typów środków przekazywania w ramach organizacji oraz między organizacją a innymi stronami. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-05-U - Procedura udostępniania danych; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników; SZBI-30-P - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			dostawców.	
A.5.15	Kontrola dostępu	Należy ustanowić i wdrożyć zasady dostępu fizycznego i logicznego do informacji i innych powiązanych aktywów na podstawie wymagań biznesowych oraz wymagań bezpieczeństwa informacji.	Tak, zabezpieczenie wdrożono. W Szpital ustanowiono i wdrożono zasady dostępu fizycznego i logicznego do informacji i innych powiązanych aktywów na podstawie wymagań biznesowych oraz wymagań bezpieczeństwa informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-04-U - Procedura nadawania upoważnień; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich; SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego; SZBI-23-U - Procedura zarządzania kluczami; SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu; SZBI-25-U - Procedura dostępu do serwerowni; SZBI-26-U - Procedura zarządzania systemem monitoringu wizyjnego.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
A.5.16	Zarządzanie tożsamością	Należy zarządzać pełnym cyklem życia tożsamości.	Tak, zabezpieczenie wdrożono. Szpital zarządza pełnym cyklem życia tożsamości. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	Nie dotyczy
A.5.17	Informacje uwierzytelniające	Przydzielanie informacji uwierzytelniających i zarządzanie nimi powinno podlegać kontroli w ramach procesu zarządzania, w tym obejmującego doradzanie personelowi w zakresie odpowiedniego postępowania z informacjami uwierzytelniającymi.	Tak, zabezpieczenie wdrożono. Przydzielanie informacji uwierzytelniających i zarządzanie nimi w Szpital podlega kontroli w ramach procesu zarządzania, w tym obejmującego doradzanie personelowi w zakresie odpowiedniego postępowania z informacjami uwierzytelniającymi. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-04-U - Procedura nadawania upoważnień; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	Nie dotyczy
A.5.18	Prawa dostępu	Należy przydzielać, przeglądać, modyfikować i odbierać prawa dostępu do informacji i innych powiązanych aktywów zgodnie z polityką tematyczną oraz zasadami organizacji dotyczącymi kontroli dostępu.	Tak, zabezpieczenie wdrożono. Szpital przydziela, przegląda, modyfikuje i odbiera prawa dostępu do informacji i innych powiązanych aktywów zgodnie z polityką tematyczną oraz zasadami organizacji	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			dotyczącymi kontroli dostępu. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-04-U - Procedura nadawania upoważnień; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	
A.5.19	Bezpieczeństwo informacji w relacjach z dostawcami	Należy opracować i wdrożyć procesy i procedury zarządzania ryzykami w bezpieczeństwie informacji związanymi z użyciem produktów lub usług dostawcy.	Tak, zabezpieczenie wdrożono. W Szpital opracowano i wdrożono procesy i procedury zarządzania ryzykami w bezpieczeństwie informacji związanymi z użyciem produktów lub usług dostawcy. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji.	Nie dotyczy
A.5.20	Uwzględnianie bezpieczeństwa informacji w porozumieniach z dostawcami	Należy ustanowić istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym dostawcą, w zależności od typu relacji z dostawcą.	Tak, zabezpieczenie wdrożono. Szpital ustanowił istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnił je z każdym dostawcą, w zależności od typu relacji z dostawcą. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			SZBI-18-U - Procedura zarządzania zmianą IT; SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników; SZBI-30-P - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców; SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.	
A.5.21	Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii teleinformatycznych (ICT)	Należy opracować i wdrożyć procesy i procedury zarządzania ryzykami w bezpieczeństwie informacji związanymi z łańcuchem dostaw produktów i usług ICT.	Tak, zabezpieczenie wdrożono. W Szpital opracowano i wdrożono procesy i procedury zarządzania ryzykami w bezpieczeństwie informacji związanymi z łańcuchem dostaw produktów i usług ICT. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-18-U - Procedura zarządzania zmianą IT; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej; SZBI-33-U – Procedura audytów wewnętrznych SZBI.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
A.5.22	Monitorowanie, przegląd i zarządzanie zmianami w usługach świadczonych przez dostawców	Organizacja powinna regularnie monitorować, przeglądać, oceniać zmiany praktyk w zakresie bezpieczeństwa informacji dostawcy i w świadczeniu usług oraz zarządzać tymi zmianami.	Tak, zabezpieczenie wdrożono. Szpital regularnie monitoruje, przegląda, ocenia zmiany praktyk w zakresie bezpieczeństwa informacji dostawcy i w świadczeniu usług oraz zarządza tymi zmianami. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital; SZBI-18-U - Procedura zarządzania zmianą IT; SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników; SZBI-30-P - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców; SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.5.23	Bezpieczeństwo informacji dotyczące stosowania usług w chmurze	Należy ustanowić procesy pozyskiwania usług w chmurze, zarządzania nimi, użycia i rezygnacji z nich zgodnie z wymaganiami bezpieczeństwa informacji w organizacji.	Tak, zabezpieczenie wdrożono. W Szpital ustanowiono procesy pozyskiwania usług w chmurze, zarządzania nimi, użycia i rezygnacji z nich zgodnie z wymaganiami bezpieczeństwa informacji w Szpital. Dokument tematyczny stanowi:	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	
A.5.24	Planowanie i przygotowanie do zarządzania incydentami związanymi z bezpieczeństwem informacji	Organizacja powinna zaplanować zarządzanie incydentami związanymi z bezpieczeństwem informacji poprzez zdefiniowanie, ustanowienie i zakomunikowanie procesów, ról i odpowiedzialności w zarządzaniu incydentami związanymi z bezpieczeństwem informacji oraz powinna przygotować się do tego zarządzania.	Tak, zabezpieczenie wdrożono. Szpital zaplanował zarządzanie incydentami związanymi z bezpieczeństwem informacji poprzez zdefiniowanie, ustanowienie i zakomunikowanie procesów, ról i odpowiedzialności w zarządzaniu incydentami związanymi z bezpieczeństwem informacji oraz przygotował się do tego zarządzania. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-10-Z - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji.	Nie dotyczy
A.5.25	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Organizacja powinna oceniać zdarzenia związane z bezpieczeństwem informacji i podjąć decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji.	Tak, zabezpieczenie wdrożono. Szpital ocenia zdarzenia związane z bezpieczeństwem informacji i podejmuje decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji. Dokument tematyczny stanowi:	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-10-Z - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji.	
A.5.26	Reagowanie na incydenty związane z bezpieczeń-stwem informacji	Reakcja na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami.	Tak, zabezpieczenie wdrożono. Reakcja na incydenty związane z bezpieczeństwem informacji w Szpital jest zgodna z udokumentowanymi procedurami. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-10-Z - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji.	Nie dotyczy
A.5.27	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informa-cji	Wiedzę zdobytą w związku z incydentami związanymi z bezpieczeństwem informacji należy wykorzystywać do wzmocnienia i poprawienia zabezpieczeń informacji.	Tak, zabezpieczenie wdrożono. Wiedzę zdobytą w związku z incydentami związanymi z bezpieczeństwem informacji Szpital wykorzystuje do wzmocnienia i poprawienia zabezpieczeń informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatno-ściami; SZBI-10-Z - Procedura zarządzania incydentami	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			związanymi z bezpieczeństwem informacji.	
A.5.28	Gromadzenie materiału dowodowego	Organizacja powinna ustanowić i wdrożyć procedury identyfikacji, gro- madzenia, pozyskiwania i utrwalania materiału dowodowego dotyczącego zdarzeń związanych z bezpieczeństwem informacji.	Tak, zabezpieczenie wdrożono. Szpital ustanowił i wdrożył procedury identyfikacji, gro-madzenia, pozyskiwania i utrwalania materiału dowodowego dotyczącego zdarzeń związanych z bezpieczeństwem informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-10-Z - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji; SZBI-33-U – Procedura audytów wewnętrznych SZBI.	Nie dotyczy
A.5.29	Bezpieczeństwo informacji podczas zakłóceń	Organizacja powinna zaplanować, jak utrzymywać bezpieczeństwo informacji na właściwym poziomie podczas zakłóceń.	Tak, zabezpieczenie wdrożono. Szpital zaplanował, jak utrzymywać bezpieczeństwo informacji na właściwym poziomie podczas zakłóceń. Dokument tematyczny stanowi: SZBI-03-P - Polityka ciągłości działania; SZBI-10-Z - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji; SZBI-11-U - Procedura użytkowania sieci telein-formatycznej; SZBI-16-Z - Procedura wykonywania kopii zapa-sowych;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.5.30	Gotowość ICT do zapewnienia ciągłości działania	Gotowość ICT powinna być zaplanowana, wdrożona, utrzymywana i testowana na podstawie celów dotyczących ciągłości działania i wymagań ciągłości ICT.	Tak, zabezpieczenie wdrożono. Gotowość ICT w Szpital jest zaplanowana, wdrożona, utrzymywana i testowana na podstawie celów dotyczących ciągłości działania i wymagań ciągłości ICT. Dokument tematyczny stanowi: SZBI-03-P - Polityka ciągłości działania; SZBI-10-Z - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-16-Z - Procedura wykonywania kopii zapasowych; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.5.31	Wymagania prawne, regulacyjne i umowne	Wymagania prawne, regulacyjne i umowne, właściwe dla bezpieczeństwa informacji, oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować.	Tak, zabezpieczenie wdrożono. Wymagania prawne, regulacyjne i umowne, właściwe dla bezpieczeństwa informacji, oraz podejście organizacji do ich przestrzegania Szpital zidentyfikował, udokumentował i na bieżąco aktualizuje. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			SZBI-02-U - Polityka ochrony danych osobowych; SZBI-03-P - Polityka ciągłości działania; SZBI-06-U - Procedura powierzenia przetwarzania danych; SZBI-07-U - Procedura oceny skutków; SZBI-13-U - Procedura pracy zdalnej; SZBI-18-U - Procedura zarządzania zmianą IT; SZBI-19-U - Procedura privacy by design, privacy by default; SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników; SZBI-30-P - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców; SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej; SZBI-33-U – Procedura audytów wewnętrznych SZBI.	
A.5.32	Prawa własności intelektualnej	Organizacja powinna wdrożyć odpowiednie procedury ochrony praw własności intelektualnej.	Tak, zabezpieczenie wdrożono. Szpital wdrożyła odpowiednie procedury ochrony praw własności intelektualnej. Dokument tematyczny stanowi:	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-12-U - Procedura rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi; SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników; SZBI-30-P - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców; SZBI-33-U – Procedura audytów wewnętrznych SZBI.	
A.5.33	Ochrona zapisów	Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem.	Tak, zabezpieczenie wdrożono. Szpital chroni zapisy przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
A.5.34	Prywatność i ochrona danych identyfikujących osobę (PII)	Organizacja powinna zidentyfikować i przestrzegać wymagań dotyczących zachowania prywatności i ochrony PII zgodnie z mającymi zastosowanie przepisami prawa i regulacjami oraz wymaganiami umownymi.	Tak, zabezpieczenie wdrożono. Szpital zidentyfikował i przestrzega wymagań dotyczących zachowania prywatności i ochrony PII zgodnie z mającymi zastosowanie przepisami prawa i regulacjami oraz wymaganiami umownymi. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-04-U - Procedura nadawania upoważnień; SZBI-05-U - Procedura udostępniania danych; SZBI-06-U - Procedura powierzenia przetwarzania danych; SZBI-07-U - Procedura oceny skutków; SZBI-19-U - Procedura privacy by design, privacy by default	Nie dotyczy
A.5.35	Niezależny przegląd bezpieczeństwa informacji	Podejście organizacji do zarządzania bezpieczeństwem informacji oraz jego wdrożenie, w tym osoby, procesy i technologie, należy poddawać nie- zależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany.	Tak, zabezpieczenie wdrożono. Podejście Szpital do zarządzania bezpieczeństwem informacji oraz jego wdrożenie, w tym osoby, procesy i technologie, Szpital poddaje się niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-18-U - Procedura zarządzania zmianą IT;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji; SZBI-33-U – Procedura audytów wewnętrznych SZBI.	
A.5.36	Zgodność z politykami, zasadami i standardami dotyczącymi bezpieczeństwa informacji	Należy regularnie poddawać przeglądom zgodność z polityką bezpieczeństwa informacji, politykami tematycznymi, zasadami i standardami organizacji.	Tak, zabezpieczenie wdrożono. Szpital regularnie poddaje przeglądom zgodność z polityką bezpieczeństwa informacji, politykami tematycznymi, zasadami i standardami organizacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-31-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji; SZBI-33-U – Procedura audytów wewnętrznych SZBI.	Nie dotyczy
A.5.37	Udokumentowane procedury eksploatacyjne	Procedury eksploatacyjne dotyczące środków przetwarzania informacji po- winny być udokumentowane i udostępniane personelowi, który ich potrzebuje.	Tak, zabezpieczenie wdrożono. Procedury eksploatacyjne dotyczące środków przetwarzania informacji w Szpital są udokumentowane i udostępniane personelowi, który ich potrzebuje. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-03-P - Polityka ciągłości działania; SZBI-04-U - Procedura nadawania upoważnień;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-13-U - Procedura pracy zdalnej; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	
A.6.	Zabezpieczenia osobowe			
A.6.1	Postępowanie sprawdzające	Historię wszystkich kandydatów, którzy mają stać się personelem, należy zweryfikować przed dołączeniem do organizacji i na bieżąco weryfikować, uwzględniając mające zastosowanie przepisy prawa, regulacje i zasady etyczne, oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp, oraz dostrzeżonych ryzyk.	Tak, zabezpieczenie wdrożono. Historię wszystkich kandydatów, którzy mają stać się personelem, Szpital weryfikuje przed dołączeniem do Szpital i na bieżąco weryfikuje, uwzględniając mające zastosowanie przepisy prawa, regulacje i zasady etyczne, oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp, oraz dostrzeżonych ryzyk. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
A.6.2	Warunki zatrudnienia	W umowach zatrudnienia należy określić odpowiedzialność personelu i organizacji dotyczące bezpieczeństwa informacji.	Tak, zabezpieczenie wdrożono. W umowach zatrudnienia Szpital określa odpowiedzialność personelu i organizacji dotyczące bezpieczeństwa informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-04-U - Procedura nadawania upoważnień; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	Nie dotyczy
A.6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Personel organizacji oraz właściwe strony zainteresowane powinny zostać odpowiednio uświadomione, odbyć stosowne kształcenie i szkolenie w zakresie bezpieczeństwa informacji oraz regularnie otrzymywać aktualizację polityki bezpieczeństwa informacji, polityk tematycznych i procedur organizacji, odpowiednio do stanowiska pracy.	Tak, zabezpieczenie wdrożono. Personel Szpital oraz właściwe strony zainteresowane zostają odpowiednio uświadomione, odbywają stosowne kształcenie i szkolenie w zakresie bezpieczeństwa informacji oraz regularnie otrzymują aktualizację polityki bezpieczeństwa informacji, polityk tematycznych i procedur organizacji, odpowiednio do stanowiska pracy. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-08-U - Procedura zarządzania ryzykiem	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			bezpieczeństwa informacji; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	
A.6.4	Postępowanie dyscyplinarne	Postępowanie dyscyplinarne powinno być sformalizowane i zakomunikowane w celu podjęcia działań wobec personelu i innych właściwych stron zainteresowanych, które naruszają politykę bezpieczeństwa informacji.	Tak, zabezpieczenie wdrożono. Postępowanie dyscyplinarne jest w Szpital sformalizowane i zakomunikowane w celu podjęcia działań wobec personelu i innych właściwych stron zainteresowanych, które naruszają politykę bezpieczeństwa informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	Nie dotyczy
A.6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia	Odpowiedzialność i obowiązki w zakresie bezpieczeństwa informacji, które pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, powinny być określone, egzekwowane i zakomunikowane właściwemu personelowi i innym stronom zainteresowanym.	Tak, zabezpieczenie wdrożono. Odpowiedzialność i obowiązki w zakresie bezpieczeństwa informacji, które pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, są w Szpital określone, egzekwowane i zakomunikowane właściwemu personelowi i innym stronom zainteresowanym. Dokument tematyczny stanowi:	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich.	
A.6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji	Umowy o zachowaniu poufności lub nieujawnianiu informacji, odzwierciedlające potrzeby organizacji dotyczące ochrony informacji, powinny być zidentyfikowane, udokumentowane, regularnie przeglądane i podpisane przez personel i inne właściwe strony zainteresowane.	Tak, zabezpieczenie wdrożono. Umowy o zachowaniu poufności lub nieujawnianiu informacji, odzwierciedlające potrzeby Szpital dotyczące ochrony informacji, są zidentyfikowane, udokumentowane, regularnie przeglądane i podpisane przez personel i inne właściwe strony zainteresowane. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich; SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników; SZBI-30-P - Procedura bezpieczeństwa w rela-	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			cjach z podmiotami zewnętrznymi dla dostawców.	
A.6.7	Praca zdalna	Należy wdrożyć zabezpieczenie, gdy personel pracuje zdalnie, żeby chronić informacje pobierane, przetwarzane lub przechowywane poza siedzibą organizacji.	Tak, zabezpieczenie wdrożono. W Szpital wdrożono zabezpieczenie, gdy personel pracuje zdalnie, żeby chronić informacje pobierane, przetwarzane lub przechowywane poza siedzibą organizacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-13-U - Procedura pracy zdalnej; SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital.	Nie dotyczy
A.6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Organizacja powinna zapewnić personelowi mechanizm niezwłocznego zgłaszania zaobserwowanych lub podejrzewanych zdarzeń związanych z bezpieczeństwem informacji za pośrednictwem odpowiednich kanałów.	Tak, zabezpieczenie wdrożono. Szpital zapewnił personelowi mechanizm niezwłocznego zgłaszania zaobserwowanych lub podejrzewanych zdarzeń związanych z bezpieczeństwem informacji za pośrednictwem odpowiednich kanałów. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-10-Z - Procedura zarządzania incydentami	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			związanymi z bezpieczeństwem informacji.	
A.7	Zabezpieczenia fizyczne			
A.7.1	Fizyczne granice obszaru bezpiecznego	Należy określić granice bezpieczeństwa i wykorzystać je do zabezpieczenia obszarów zawierających informacje i inne powiązane aktywa.	Tak, zabezpieczenie wdrożono. W Szpital określono granice bezpieczeństwa i wykorzystania ich do zabezpieczenia obszarów zawierających informacje i inne powiązane aktywa. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego; SZBI-23-U - Procedura zarządzania kluczami; SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu; SZBI-25-U - Procedura dostępu do serwerowni; SZBI-26-U - Procedura zarządzania systemem monitoringu wizyjnego.	Nie dotyczy
A.7.2	Wejście fizyczne	Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść i punktami dostępu.	Tak, zabezpieczenie wdrożono. Bezpieczne strefy są w Szpital chronione odpowiednimi	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			zabezpieczeniami wejść i punktami dostępu. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego; SZBI-23-U - Procedura zarządzania kluczami; SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu; SZBI-25-U - Procedura dostępu do serwerowni; SZBI-26-U - Procedura zarządzania systemem monitoringu wizyjnego.	
A.7.3	Zabezpieczenie biur, pomieszczeń i obiektów	Należy zaprojektować i wdrożyć fizyczne zabezpieczenie biur, pomieszczeń i obiektów.	Tak, zabezpieczenie wdrożono. W Szpital zaprojektowano i wdrożono fizyczne zabezpieczenie biur, pomieszczeń i obiektów. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego; SZBI-23-U - Procedura zarządzania kluczami; SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu; SZBI-25-U - Procedura dostępu do serwerowni;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			SZBI-26-U - Procedura zarządzania systemem monitoringu wizyjnego.	
A.7.4	Monitorowanie bezpieczeństwa fizycznego	Pomieszczenia powinny być stale monitorowane pod kątem nieuprawnionego dostępu fizycznego.	Tak, zabezpieczenie wdrożono. Pomieszczenia w Szpital są stale monitorowane pod kątem nieuprawnionego dostępu fizycznego. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego; SZBI-23-U - Procedura zarządzania kluczami; SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu; SZBI-25-U - Procedura dostępu do serwerowni; SZBI-26-U - Procedura zarządzania systemem monitoringu wizyjnego.	Nie dotyczy
A.7.5	Ochrona przed zagrożeniami fizycznymi i środowiskowymi	Należy zaprojektować i wdrożyć ochronę przed zagrożeniami fizycznymi i środowiskowymi, takimi jak katastrofy naturalne lub inne zamierzone lub niezamierzone zagrożenia fizyczne dla infrastruktury.	Tak, zabezpieczenie wdrożono. W Szpital zaprojektowano i wdrożono ochronę przed zagrożeniami fizycznymi i środowiskowymi, takimi jak katastrofy naturalne lub inne zamierzone lub niezamierzone zagrożenia fizyczne dla infrastruktury. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego; SZBI-23-U - Procedura zarządzania kluczami; SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu; SZBI-25-U - Procedura dostępu do serwerowni.	
A.7.6	Praca w obszarach bezpiecznych	Należy zaprojektować i wdrożyć środki bezpieczeństwa dotyczące pracy w obszarach bezpiecznych.	Tak, zabezpieczenie wdrożono. W Szpital zaprojektowano i wdrożono środki bezpieczeństwa dotyczące pracy w obszarach bezpiecznych. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego; SZBI-23-U - Procedura zarządzania kluczami; SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu; SZBI-25-U - Procedura dostępu do serwerowni; SZBI-26-U - Procedura zarządzania systemem monitoringu wizyjnego.	Nie dotyczy
A.7.7	Czyste biurko i czysty ekran	Należy opracować i właściwie egzekwować zasady czystego biurka dla dokumentów papierowych i przenośnych nośników informacji oraz zasady czystego ekranu dla środków przetwarzania informacji.	Tak, zabezpieczenie wdrożono. W Szpital opracowano i właściwie egzekwuje się zasady czystego biurka dla dokumentów papierowych i przenośnych nośników informacji oraz zasady czystego ekranu dla środków przetwarzania	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi.	
A.7.8	Lokalizacja i ochrona sprzętu	Należy sprzęt umieścić w bezpiecznym miejscu i chronić.	Tak, zabezpieczenie wdrożono. W Szpital sprzęt umieszczany jest w bezpiecznym miejscu i jest chroniony. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-17-U - Procedura rejestracji i inwentaryzacji sprzętu i wyposażenia; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi.	Nie dotyczy
A.7.9	Bezpieczeństwo aktywów poza siedzibą	Należy chronić aktywa poza siedzibą.	Tak, zabezpieczenie wdrożono. Szpital chroni aktywa poza siedzibą. Dokument tematyczny stanowi:	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-17-U - Procedura rejestracji i inwentaryzacji sprzętu i wyposażenia; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi.	
A.7.10	Nośniki informacji	Należy zarządzać nośnikami informacji przez cały cykl ich życia: pozyskanie, użycie, transportowanie i zbycie, zgodnie ze schematem klasyfikacji organizacji oraz wymaganiami dotyczącymi postępowania.	Tak, zabezpieczenie wdrożono. Szpital zarządza nośnikami informacji przez cały cykl ich życia: pozyskanie, użycie, transportowanie i zbycie, zgodnie ze schematem klasyfikacji organizacji oraz wymaganiami dotyczącymi postępowania. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-17-U - Procedura rejestracji i inwentaryzacji sprzętu i wyposażenia; SZBI-20-U - Procedura zarządzania aktywami informacyjnymi; SZBI-32-Z - Procedura ciągłości działania sieci	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			teleinformatycznej.	
A.7.11	Systemy wspomagające	Środki przetwarzania informacji należy chronić przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających.	Tak, zabezpieczenie wdrożono. Środki przetwarzania informacji Szpital chroni przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-02-U - Polityka ochrony danych osobowych; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.7.12	Bezpieczeństwo okablowania	Okablowanie zasilające, sygnałowe lub wspomagające usługi informacyjne należy chronić przed przechwyceniem, zakłóceniem lub uszkodzeniem.	Tak, zabezpieczenie wdrożono. Okablowanie zasilające, sygnałowe lub wspomagające usługi informacyjne są w Szpital chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.7.13	Konserwacja sprzętu	Sprzęt należy prawidłowo utrzymywać w celu zapewnienia dostępności, integralności i poufności informacji.	Tak, zabezpieczenie wdrożono. Sprzęt w Szpital jest prawidłowo utrzymywany w celu zapewnienia dostępności, integralności i poufności informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-15-Z - Procedura przechowywania i przekazywania hasła administratora systemu; SZBI-16-Z - Procedura wykonywania kopii zapasowych; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.7.14	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy sprawdzić jego składniki zawierające nośniki informacji, aby upewnić się, czy wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.	Tak, zabezpieczenie wdrożono. Przed zbyciem lub przekazaniem sprzętu do ponownego użycia Szpital sprawdza jego składniki zawierające nośniki informacji, aby upewnić się, czy wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	
A.8	**Zabezpieczenia technologiczne**			
A.8.1	Urządzenia końcowe użytkownika	Należy chronić informacje przechowywane, przetwarzane lub dostępne przez urządzenia końcowe użytkownika.	Tak, zabezpieczenie wdrożono. W Szpital chroni się informacje przechowywane, przetwarzane lub dostępne przez urządzenia końcowe użytkownika. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	Nie dotyczy
A.8.2	Prawa uprzywilejowanego dostępu	Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczać i nimi zarządzać.	Tak, zabezpieczenie wdrożono. W Szpital przydzielanie i wykorzystanie praw uprzywilejowanego dostępu ogranicza się i nimi zarządza. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-14-U - Procedura dostępu VPN do zaso-	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			bów sieci Szpital; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	
A.8.3	Ograniczanie dostępu do informacji	Dostęp do informacji i innych powiązanych aktywów należy ograniczać zgodnie z ustanowioną polityką tematyczną dotyczącą kontroli dostępu.	Tak, zabezpieczenie wdrożono. Dostęp do informacji i innych powiązanych aktywów Szpital ograniczył zgodnie z ustanowioną polityką tematyczną dotyczącą kontroli dostępu. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	Nie dotyczy
A.8.4	Dostęp do kodu źródłowego	Należy właściwie zarządzać dostępem w trybie „odczytu” i „zapisu” do kodu źródłowego, narzędzi programistycznych i bibliotek oprogramowania.	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz nie prowadzi prac rozwojowych systemów informacyjnych.
A.8.5	Bezpieczne uwierzytelnianie	Powinny być wdrożone techniki i procedury bezpiecznego uwierzytelniania zgodnie z ograniczeniami dostępu do informacji i polityką tematyczną dotyczącą kontroli dostępu.	Tak, zabezpieczenie wdrożono. W Szpital wdrożono techniki i procedury bezpiecznego uwierzytelniania zgodnie z ograniczeniami dostępu do informacji i polityką tematyczną dotyczącą kontroli dostępu. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	
A.8.6	Zarządzanie pojemnością	Należy monitorować i regulować wykorzystywanie zasobów zgodnie z obecnymi i przewidywanymi wymaganiami dotyczącymi pojemności.	Tak, zabezpieczenie wdrożono. W Szpital monitoruje się i reguluje wykorzystywanie zasobów zgodnie z obecnymi i przewidywanymi wymaganiami dotyczącymi pojemności. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.7	Ochrona przed szkodliwym oprogramowaniem	Należy wdrożyć ochronę przed szkodliwym oprogramowaniem i wspierać ją przez właściwą świadomość użytkowników.	Tak, zabezpieczenie wdrożono. W Szpital wdrożono ochronę przed szkodliwym oprogramowaniem i wspiera się ją przez właściwą świadomość użytkowników. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-03-P - Polityka ciągłości działania; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-14-U - Procedura dostępu VPN do zasobów sieci Szpital; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.8.8	Zarządzanie podatnościami technicznymi	Należy pozyskiwać informacje o podatnościach technicznych używanych systemów informacyjnych, należy oceniać narażenia organizacji przez te podatności i podejmować odpowiednie środki.	Tak, zabezpieczenie wdrożono. Szpital pozyskuje informacje o podatnościach technicznych używanych systemów informacyjnych, ocenia narażenia organizacji przez te podatności i podejmować odpowiednie środki. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			teleinformatycznej.	
A.8.9	Zarządzanie konfiguracją	Należy ustanowić, udokumentować, wdrożyć, monitorować i poddawać przeglądom konfiguracje, w tym konfiguracje bezpieczeństwa, sprzętu, oprogramowania, usług i sieci.	Tak, zabezpieczenie wdrożono. Szpital ustanowił, udokumentował, wdrożył, monitoruje i poddaje przeglądom konfiguracje, w tym konfiguracje bezpieczeństwa, sprzętu, oprogramowania, usług i sieci. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.10	Usuwanie informacji	Należy usuwać informacje przechowywane w systemach informacyjnych, na urządzeniach lub na jakichkolwiek innych nośnikach informacji, kiedy już nie są wymagane.	Tak, zabezpieczenie wdrożono. W Szpital usuwa się informacje przechowywane w systemach informacyjnych, na urządzeniach lub na jakichkolwiek innych nośnikach informacji, kiedy już nie są wymagane. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-03-P - Polityka ciągłości działania; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.8.11	Maskowanie danych	Maskowania danych należy używać zgodnie z polityką tematyczną organizacji dotyczącą kontroli dostępu i innymi powiązanymi politykami tematycznymi oraz z wymaganiami biznesowymi, biorąc pod uwagę mające zastosowanie przepisy prawa.	Tak, zabezpieczenie wdrożono. Maskowania danych w Szpital używa się zgodnie z polityką tematyczną organizacji dotyczącą kontroli dostępu i innymi powiązanymi politykami tematycznymi oraz z wymaganiami biznesowymi, biorąc pod uwagę mające zastosowanie przepisy prawa. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-07-U - Procedura oceny skutków; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-19-U - Procedura privacy by design, privacy by default.	
A.8.12	Zapobieganie wyciekom danych	Środki zapobiegania wyciekom danych należy stosować w systemach, sieciach i innych urządzeniach, które przetwarzają, przechowują lub przesyłają informacje wrażliwe.	Tak, zabezpieczenie wdrożono. Środki zapobiegania wyciekom danych Szpital stosuje w systemach, sieciach i innych urządzeniach, które przetwarzają, przechowują lub przesyłają informacje wrażliwe. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.13	Zapasowe kopie informacji	Zapasowe kopie informacji, oprogramowania i systemów należy utrzymywać i regularnie testować, zgodnie z ustaloną polityką tematyczną dotyczącą kopii zapasowych.	Tak, zabezpieczenie wdrożono. Zapasowe kopie informacji, oprogramowania i systemów Szpital utrzymuje i regularnie testuje, zgodnie z ustaloną polityką tematyczną dotyczącą kopii zapasowych. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji;	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-16-Z - Procedura wykonywania kopii zapasowych; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.8.14	Nadmiarowość środków przetwarzania informacji	Środki przetwarzania informacji należy wdrażać z nadmiarowością wystarczającą do spełnienia wymagań dostępności.	Tak, zabezpieczenie wdrożono. Środki przetwarzania informacji Szpital wdraża z nadmiarowością wystarczającą do spełnienia wymagań dostępności. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-07-U - Procedura oceny skutków; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.15	Rejestrowanie	Należy opracowywać, przechowywać, chronić i analizować dzienniki zdarzeń, rejestrujące działania, wyjątki, usterki i inne istotne zdarzenia.	Tak, zabezpieczenie wdrożono. Szpital opracowywał, przechowuje, chroni i analizuje dzienniki zdarzeń, rejestrujące działania, wyjątki, usterki i inne istotne zdarzenia.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
			Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.8.16	Działania monitorujące	Sieci, systemy i aplikacje należy monitorować pod kątem nietypowego zachowania i podejmować odpowiednie działania w celu oceny potencjalnych incydentów związanych z bezpieczeństwem informacji.	Tak, zabezpieczenie wdrożono. Sieci, systemy i aplikacje w Szpital monitoruje się pod kątem nietypowego zachowania i podejmuje się odpowiednie działania w celu oceny potencjalnych incydentów związanych z bezpieczeństwem informacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji; SZBI-09-Z - Procedura zarządzania podatnościami; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
A.8.17	Synchronizacja zegarów	Zegary systemów przetwarzania informacji wykorzystywanych w organizacji należy zsynchronizować z zatwierdzonymi źródłami czasu.	Tak, zabezpieczenie wdrożono. Zegary systemów przetwarzania informacji wykorzystywanych w Szpital są zsynchronizowane z zatwierdzonymi źródłami czasu. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.18	Użycie uprzywilejowanych programów narzędziowych	Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi.	Tak, zabezpieczenie wdrożono. Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, podlega w Szpital ograniczeniom i ścisłemu nadzorowi. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.19	Instalacja oprogramowania w	Należy wdrożyć procedury i środki bezpiecznego zarządzania instalacją	Tak, zabezpieczenie wdrożono. W Szpital wdrożono procedury i środki bezpiecznego	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
	systemach produkcyjnych	oprogramowania w systemach produkcyjnych.	zarządzania instalacją oprogramowania w systemach produkcyjnych. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.8.20	Bezpieczeństwo sieci	Sieci i urządzenia sieciowe powinny być zabezpieczone, zarządzane i nadzorowane w celu ochrony informacji w systemach i aplikacjach.	Tak, zabezpieczenie wdrożono. Sieci i urządzenia sieciowe w Szpital są zabezpieczone, zarządzane i nadzorowane w celu ochrony informacji w systemach i aplikacjach. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.21	Bezpieczeństwo usług sieciowych	Należy zidentyfikować, wdrożyć i monitorować mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania serwisowe dla usług sieciowych.	Tak, zabezpieczenie wdrożono. Szpital zidentyfikował, wdrożył i monitoruje mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania serwisowe dla usług sieciowych. Dokument tematyczny stanowi:	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	
A.8.22	Rozdzielanie sieci	Grupy usług informacyjnych, użytkowników i systemów informacyjnych powinny być rozdzielone w strukturze sieci organizacji.	Tak, zabezpieczenie wdrożono. Grupy usług informacyjnych, użytkowników i systemów informacyjnych są w Szpital rozdzielone w strukturze sieci organizacji. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.23	Filtrowanie treści internetowych	Należy zarządzać dostępem do zewnętrznych stron internetowych, aby ograniczyć narażenie na szkodliwe treści.	Tak, zabezpieczenie wdrożono. Szpital zarządza dostępem do zewnętrznych stron internetowych, aby ograniczyć narażenie na szkodliwe treści. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
			teleinformatycznej.	
A.8.24	Użycie kryptografii	Należy opracować i wdrożyć zasady skutecznego używania kryptografii, w tym zarządzania kluczami kryptograficznymi.	Tak, zabezpieczenie wdrożono. W Szpital opracowano i wdrożono zasady skutecznego używania kryptografii, w tym zarządzania kluczami kryptograficznymi. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej.	Nie dotyczy
A.8.25	Bezpieczne wytwarzanie oprogramowania	Należy ustanowić i stosować zasady bezpiecznego wytwarzania oprogramowania i systemów.	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz nie prowadzi prac rozwojowych systemów informacyjnych.
A.8.26	Wymagania bezpieczeństwa aplikacji	Należy zidentyfikować, określić i zatwierdzić wymagania bezpieczeństwa informacji podczas wytwarzania lub pozyskiwania aplikacji.	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz nie prowadzi prac rozwojowych systemów informacyjnych.
A.8.27	Zasady bezpiecznej architektury systemu i jej projektowania	Należy ustanowić, udokumentować i utrzymywać zasady projektowanie bezpiecznych systemów oraz stosować je do	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz nie prowadzi prac rozwojowych systemów

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
		wszystkich działań dotyczących wytwarzania systemów informacyjnych.		informacyjnych.
A.8.28	Bezpieczne kodowanie	Przy wytwarzaniu oprogramowania należy stosować zasady bezpiecznego kodowania.	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz nie prowadzi prac rozwojowych systemów informacyjnych.
A.8.29	Testowanie bezpieczeństwa podczas wytwarzania i akceptowania	Procesy testowania bezpieczeństwa powinny być opracowane i wdrożone w całym cyklu wytwarzania.	Tak, zabezpieczenie wdrożono. Procesy testowania bezpieczeństwa w Szpital są opracowane i wdrożone w całym cyklu wytwarzania. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-07-U - Procedura oceny skutków; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-16-Z - Procedura wykonywania kopii zapasowych; SZBI-18-U - Procedura zarządzania zmianą IT; SZBI-19-U - Procedura privacy by design, privacy by default; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy

Wykaz niezbędnych zabezpieczeń		Uzasadnienie wyboru zabezpieczenia	Stwierdzenie czy niezbędne zabezpieczenia są wdrożone	Uzasadnienie pominięcia zabezpieczenia
A.8.30	Wytwarzanie zlecane podmiotom zewnętrznym	Organizacja powinna kierować, monitorować i poddawać przeglądom działania związane z wytwarzaniem systemów zlecanym podmiotom zewnętrznym.	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz nie prowadzi prac rozwojowych systemów informacyjnych.
A.8.31	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Należy oddzielać i zabezpieczać środowiska rozwojowe, testowe i produkcyjne.	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz nie prowadzi prac rozwojowych systemów informacyjnych.
A.8.32	Zarządzanie zmianami	Zmiany w środkach przetwarzania informacji i systemach informacyjnych powinny podlegać procedurom zarządzania zmianami.	Tak, zabezpieczenie wdrożono. W Szpital zmiany w środkach przetwarzania informacji i systemach informacyjnych podlegają procedurom zarządzania zmianami. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-07-U - Procedura oceny skutków; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-18-U - Procedura zarządzania zmianą IT; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej.	Nie dotyczy
A.8.33	Informacje testowe	Należy właściwie wybierać, chronić i zarządzać	Zabezpieczenia nie wdrożono.	Szpital nie wytwarza oprogramowania oraz

Wykaz niezbędnych zabezpieczeń		**Uzasadnienie wyboru zabezpieczenia**	**Stwierdzenie czy niezbędne zabezpieczenia są wdrożone**	**Uzasadnienie pominięcia zabezpieczenia**
		informacjami testowymi.		nie prowadzi prac rozwojowych systemów informacyjnych.
A.8.34	Ochrona systemów informacyjnych podczas testów audytowych	Testy audytowe i inne działania uzasadnienia zaufania, obejmujące ocenę systemów produkcyjnych powinny być zaplanowane i uzgodnione między testerem a właściwym kierownictwem.	Tak, zabezpieczenie wdrożono. Testy audytowe i inne działania uzasadnienia zaufania, obejmujące ocenę systemów produkcyjnych w Szpital są zaplanowane i uzgodnione między testerem a właściwym kierownictwem. Dokument tematyczny stanowi: SZBI-01-P - Polityka bezpieczeństwa informacji; SZBI-03-P - Polityka ciągłości działania; SZBI-11-U - Procedura użytkowania sieci teleinformatycznej; SZBI-16-Z - Procedura wykonywania kopii zapasowych; SZBI-18-U - Procedura zarządzania zmianą IT; SZBI-32-Z - Procedura ciągłości działania sieci teleinformatycznej; SZBI-33-U – Procedura audytów wewnętrznych SZBI.	Nie dotyczy