WŁAŚCICIEL:	ASI/ASK
Odpowiedzialny za przegląd i aktualizację dokumentu *(co najmniej raz na 3 lata):*	ASI/ASK

I. CEL

Celem instrukcji jest zapewnienie bezpieczeństwa informatycznych systemów szpitalnych, wdrażanych i rozwijanych przez wykonawców, a także bezpieczeństwa realizacji zadań na rzecz Szpitala.

II. PRZEDMIOT I ZAKRES INSTRUKCJI

Przedmiotem instrukcji jest określenie zasad postępowania oraz zakresu obowiązków i odpowiedzialności wykonawców w zakresie bezpieczeństwa informacji.
Niniejsza instrukcja obejmuje swym zakresem wszystkich wykonawców uzyskujących dostęp, przetwarzających, przechowujących, przesyłających lub dostarczających elementy infrastruktury teleinformatycznej oraz medycznej służących do przetwarzania informacji należących do Szpitala.
Niniejszy dokument dotyczy wszystkich systemów informatycznych oraz medycznych, które są wdrażane, rozwijane bądź utrzymywane, będących własnością Szpitala, lub powierzonych do użytkowania.
Postanowienia niniejszej instrukcji należy stosować we wszystkich umowach z wykonawcami, których przedmiot jest związany z ochroną informacji.

III. TERMINOLOGIA

Szpital – Wielospecjalistyczny Szpital Samodzielny Publiczny Zakład Opieki Zdrowotnej w Nowej Soli

Wykonawca – podmiot, który zobowiązuje się do realizacji określonych prac lub świadczenia usług na podstawie zawartej umowy

Administrator – osoba zajmująca się zarządzaniem systemem informatycznym

Administrator Systemów Informatycznych/Administrator Sieci Komputerowych (ASI/ASK) – osoba nadzorująca pracę systemu informatycznego i sieci komputerowej, wykonująca czynności wymagające specjalnych uprawnień.

Opracował	Administrator Systemów Informatycznych/Administrator Sieci Komputerowych	16.01.2025	Marcin Bunikiewicz Kierownik Działu Informatyki
Sprawdził - merytorycznie	Lider Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania Szpitala	16.01.25 r.	Dawid Mudaniski
Sprawdził - formalnie	Pełnomocnik Dyrektora ds. Jakości	16.01.25 r.	PEŁNOMOCNIK DYREKTORA DS. JAKOŚCI Merk
Zatwierdził	Dyrektor	17.01.2025	DYREKTOR WIELOSPECJALISTYCZNEGO SZPITALA SAMODZIELNEGO PUBLICZNEGO ZAKŁADU OPIEKI ZDROWOTNEJ w Nowej Soli Jarosław Sieracki
		DATA	PIECZĘĆ I PODPIS

IV. ODPOWIEDZIALNOŚĆ I SPOSÓB POSTĘPOWANIA

1. Postanowienia ogólne

1.1 Każdy wykonawca musi spełniać wymagania niniejszej instrukcji przed uzyskaniem dostępu do infrastruktury i systemów teleinformatycznych Szpitala.

1.2 Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych oraz wrażliwych, wykonawca musi spełniać warunki:

a) przeszkolić pracowników i osoby trzecie realizujące w jego imieniu zadania na rzecz Szpitala, w zakresie zachowania zasad bezpieczeństwa informacji,

b) każda osoba, która w imieniu wykonawcy bezpośrednio uczestniczy w realizacji przedmiotu Umowy na rzecz Szpitala zobowiązana jest do zapoznania się z niniejszą instrukcją oraz z Polityką zintegrowanego systemu zarządzania (zamieszczoną na stronie internetowej www.szpital-nowasol.pl),

c) wykonawca jest zobowiązany do pisemnego potwierdzenia zapoznania się z niniejszą instrukcją potwierdzając przyjęcie do wiadomości na formularzu Oświadczenia wykonawcy w zakresie bezpieczeństwa informacji (Adm-521),

d) w przypadku powierzenia przetwarzania danych osobowych Szpitala, podpisać Umowę powierzenia przetwarzania danych osobowych (Adm-209),

1.3 Szpital zastrzega sobie prawo do możliwości przeprowadzenia audytu Wykonawcy w celu weryfikacji zgodności z wymaganiami bezpieczeństwa zawartymi w niniejszej polityce.

2. Dostęp do środowiska teleinformatycznego

1.1 Wykonawca zobowiązany jest wykorzystywać przyznany dostęp wyłącznie w celach i w zakresie uzasadnionym realizacją zadań wynikających z przedmiotu Umowy, zgodnie z Umową oraz obowiązującymi przepisami prawa.

1.2 Wykonawca zobowiązany jest zapewnić właściwą ochronę udostępnionych mu systemów lub zasobów informacyjnych Szpitala, polegającą w szczególności na zapewnieniu środków organizacyjnych, technicznych i prawnych stosowanych w celu zapewnienia bezpieczeństwa informacji.

1.3 Dostęp do krytycznych zasobów Szpitala realizowany jest wyłącznie z użyciem stacji przesiadkowych udostępnianych przez Szpital. Sesje takie są izolowane, monitorowane i nagrywane w czasie rzeczywistym.

1.4 W uzasadnionych przypadkach istnieje możliwość odstępstwa od zapisów pkt 2.1.3.

1.5 W związku z dostępem do środowiska teleinformatycznego Szpitala, Wykonawca ma obowiązek stosować się do zaleceń oraz wymagań Szpitala mających na celu zapewnienie bezpieczeństwa informacji, w tym m.in. zapoznać własny personel i zapewnić przestrzeganie wskazanych przez Szpital zasad bezpiecznego użytkowania systemu teleinformatycznego. Wykonawca jednocześnie zapewnia, że dostęp do systemów lub zasobów teleinformatycznych Szpitala będą posiadać wyłącznie uprawnieni i przeszkoleni pracownicy/współpracownicy, w zakresie i na czas niezbędny do realizacji przez nich przedmiotu Umowy.

1.6 Bez uszczerbku dla postanowień Umowy, wykonawca ponosi pełną odpowiedzialność za działania swoich pracowników/współpracowników w systemach lub zasobach teleinformatycznych Szpitala oraz za wszelkie szkody powstałe w związku z korzystaniem przez wykonawcę z dostępu do systemów lub zasobów teleinformatycznych Szpitala w sposób sprzeczny z przedmiotem umowy oraz niniejszą instrukcją.

1.7 Bez uszczerbku dla postanowień Umowy, w sytuacji korzystania przez wykonawcę przy realizacji Umowy z usług podwykonawców, wykonawca zapewnia przestrzeganie przez te podmioty oraz osoby realizujące w ich imieniu Umowę wszystkich wymagań bezpieczeństwa Szpitala, o których mowa w niniejszej Polityce i ponosi w tym zakresie pełną odpowiedzialność względem Szpitala

3. Zarządzanie uprawnieniami

1.1 Dostęp wykonawcy do środowiska teleinformatycznego Szpitala odbywa się wyłącznie na zasadach określonych w niniejszej instrukcji.
1.2 Dostęp zdalny może być udzielony wyłącznie osobom, które zostały jednoznacznie wskazane w załączniku do umowy Zasady udzielania zdalnego dostępu do zasobów (BI-27). Osoby te otrzymują tożsamość cyfrową w systemie teleinformatycznym Szpitala.
1.3 Zakres nadawanych uprawnień jest określany na podstawie załącznika do umowy Wniosek o zmianę polityki sieciowej (BI-28).
1.4 Nadawanie, modyfikowanie oraz usuwanie użytkowników w systemie teleinformatycznym Szpitala realizowana jest przez Administratora.
1.5 Lista użytkowników ze strony wykonawcy, jest dostarczona przez osoby wskazane w Umowie, jako odpowiedzialne za jej realizację. Po każdej zmianie użytkowników ze strony wykonawcy, jest on zobowiązany do przekazania listy użytkowników ze wskazaniem zmian w zakresie ich uprawnień.
1.6 W przypadku zakończenia przez wykonawcę współpracy z pracownikiem/współpracownikiem, wykonawca bezzwłocznie informuje osoby wskazane w umowie do kontaktu ze strony szpitala o zmianach personalnych. Brak zgłoszenia zakończenia współpracy przenosi wszelką odpowiedzialność za aktywność danego użytkownika na wykonawcę.

4. Metody i środki uwierzytelniania

1.1 Dostęp do środowiska teleinformatycznego Szpitala może mieć wyłącznie użytkownik po podaniu identyfikatora (loginu) i właściwego hasła.
1.2 Dostęp do środowiska teleinformatycznego Szpitala odbywa się z wykorzystaniem mechanizmów podwójnej autentykacji.

5. Minimalne wymogi bezpieczeństwa

1.1 Wykonawca winien stosować klasyfikację informacji przesyłanej, przechowywanej i przetwarzanej w kontekście realizacji zadań na rzecz Szpitala, zgodnie z zasadami klasyfikacji opisanymi w niniejszej instrukcji.
1.2 Wykonawca jest zobowiązany do zapewnienia, przy dochowaniu najwyższej staranności, właściwej ochrony udostępnionego środowiska teleinformatycznego Szpitala, w szczególności wdrożenia po swej stronie mechanizmów organizacyjno-technicznych gwarantujących:
   a) dostęp do systemów lub zasobów teleinformatycznych wyłącznie dla uprawnionych użytkowników,
   b) rozliczalność użytkowników, rozumianą jako możliwość jednoznacznego przypisania działań prowadzonych w systemie lub zasobie do konkretnego użytkownika.
1.3 Realizując wymagania, o których mowa w pkt. 5.1.1 Wykonawca zapewni w szczególności:
   a) ochronę wszelkich udostępnionych mu przez Szpital informacji (np. loginy i hasła) przed dostępem osób nieuprawnionych,
   b) skuteczne mechanizmy organizacyjne i techniczne uniemożliwiające użytkownikom:
      - dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych Szpitala,
      - podejmowanie działań, które pośrednio lub bezpośrednio mogą prowadzić do naruszenia bezpieczeństwa udostępnionych systemów lub zasobów teleinformatycznych.
1.4 Wykonawca musi zapewnić bezpieczeństwo informacji przesyłanej, w szczególności:
   a) zapewnić ochronę poufności oraz integralności informacji przesyłanej publicznymi kanałami transmisyjnymi, odpowiednio do jej klasy bezpieczeństwa,
   b) zapewnić szyfrowanie komunikacji w oparciu o rozwiązania zapewniające poziom bezpieczeństwa, co najmniej równy temu jaki zapewniają protokoły TLS w wersji co najmniej 1.2 lub VPN.

1.5 Wykonawca musi zidentyfikować i udokumentować łańcuch dostaw związany z realizacją Umowy. Musi zapewnić, że jego podwykonawcy zapewniają taki sam poziom bezpieczeństwa jaki spełnia on sam w odniesieniu do Szpitala. Wykonawca odpowiada za zapewnienie bezpieczeństwa w całym łańcuchu dostaw produktów i usług, za który jest odpowiedzialny zgodnie z zawartą Umową.

1.6 Wykonawca winien zapewnić bezpieczeństwo nośników danych wykorzystywanych w związku z realizacją zadań na rzecz Szpitala, w szczególności musi:

a) posiadać i realizować polityki dotyczące bezpiecznego usuwania danych z nośników zawierających dane związane z realizacją zadań na rzecz Szpitala, zapewniając skuteczne usuwanie,
b) usuwać wszystkie dane szpitala zebrane podczas realizacji umowy po jej zakończeniu chyba, że zapisy umowy stanowią inaczej,
c) posiadać i realizować polityki bezpiecznego przekazywania nośników zawierających dane związane z realizacją zadań na rzecz Szpitala, zapewniając skuteczną ochronę danych.

1.7 Wszelkie oprogramowanie wykorzystywane w ramach realizacji przez wykonawcę przedmiotu Umowy musi być użytkowane z poszanowaniem praw własności intelektualnej, w szczególności zgodnie z Ustawą o prawie autorskim i prawach pokrewnych (tj. Dz.U. z 2022 r. poz. 2509 ze zm.).

6. Bezpieczeństwo infrastruktury

1.1 Do środowiska teleinformatycznego Szpitala mogą być podłączane wyłącznie komputery i urządzenia spełniające minimalne wymagania bezpieczeństwa, w szczególności:

a) system operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń,
b) zainstalowano oprogramowanie szyfrujące zawartość dysków twardych,
c) system antywirusowy jest zainstalowany w systemie operacyjnym, a jego sygnatury są aktualne,
d) firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez użytkowników komputera,
e) zainstalowane na komputerze oprogramowanie pochodzi z zaufanych źródeł,
f) oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania.

1.2 Zabrania się wykonawcy samodzielnego dokonywania zmian w konfiguracji i oprogramowaniu urządzeń udostępnionych przez Szpital.

1.3 Wszystkie czynności wykonywane przez wykonawcę w systemie informatycznym Szpitala mogą się odbywać tylko i wyłącznie po zleceniu i pod nadzorem wyznaczonych pracowników szpitala.

1.4 Urządzenia wykonawcy, służące do komunikacji ze środowiskiem teleinformatycznym Szpitala muszą być chronione w sposób uniemożliwiający bezpośrednie lub pośrednie pozyskanie przez osoby nieupoważnione dostępu do środowiska teleinformatycznego Szpitala. Wykonawca w szczególności ma obowiązek wyeliminować możliwość przejęcia kontroli nad tymi urządzeniami lub ich wykorzystania w trakcie komunikacji.

1.5 Zabrania się podejmowania prób sprawdzania, testowania i omijania zabezpieczeń systemów informatycznych Szpitala, z wyłączeniem zadań realizowanych na mocy Umowy dotyczącej przeprowadzenia autoryzowanych testów bezpieczeństwa.

7. Stosowanie zabezpieczeń kryptograficznych

1.1 W celu ochrony poufności przesyłanych oraz przechowywanych danych należy stosować zabezpieczenia kryptograficzne. Zabezpieczenia powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi, w szczególności należy stosować zabezpieczenia kryptograficzne:

a) na dyskach twardych komputerów przenośnych,
b) na pamięciach wymiennych typu pendrive, dysk zewnętrzny itp.

c) na nośnikach kopii zapasowych przechowywanych poza systemem informatycznym Szpitala,
a) tunelach VPN,
b) korespondencji elektronicznej, w trakcie przesyłania danych objętych ochroną.

1.2 Zakres stosowanych rozwiązań kryptograficznych powinien obejmować minimum dane znajdujące się na nośnikach, które objęte są ochroną ze względu na wymagania utrzymania odpowiedniego poziomu poufności.

V. ZAPISY

Lp.	Nazwa dokumentu	Forma przechowywania	Miejsce przechowywania	Czas przechowywania Minimum	Sposób postępowania po okresie przechowywania
1	Adm-521 Oświadczenia wykonawcy w zakresie bezpieczeństwa informacji	Papierowa	Dział Zamówień Publicznych	5 lat	Zgodnie z Instrukcją Kancelaryjną
2	Adm-209 Umowa powierzenia przetwarzanie danych osobowych	Papierowa	Dział Zamówień Publicznych	5 lat	Zgodnie z Instrukcją Kancelaryjną
3	BI-28 Wniosek o zmianę polityki sieciowej	Papierowa	Dział Informatyki	2 lata	Zgodnie z Instrukcją Kancelaryjną

VI. ZAŁĄCZNIKI

1. Adm-521 Oświadczenia wykonawcy w zakresie bezpieczeństwa informacji
2. Adm-209 Umowa powierzenia przetwarzanie danych osobowych
3. BI-28 Wniosek o zmianę polityki sieciowej

VII. DOKUMENTY ZWIĄZANE

1. Ustawa o prawie autorskim i prawach pokrewnych (tj. Dz.U. z 2022 r. poz. 2509 ze zm.)
2. Polityka zintegrowanego systemu zarządzania Wielospecjalistycznego Szpitala SPZOZ w Nowej Soli
3. Umowa z wykonawcą
4. BI-27 Zasady udzielenia zdalnego dostępu do zasobów