„ZASADY PRZYZNAWANIA ZDALNEGO DOSTĘPU DO URZĄDZEŃ W SIECI SZPITALNEJ FIRMOM ZEWNĘTRZNYM”

Postanowienia ogólne:

1. Przyjmujący zlecenie deklaruje, że przestrzega zaleceń dotyczących przetwarzania danych określonych w normie ISO 27001.
2. Przyjmujący zlecenie zobowiązuje się do przedstawienia kompletnej listy używanych do komunikacji portów oraz publicznych adresów IP, z których będzie realizowana usługa zdalnego serwisu. Zmiany powinny być zgłaszane najpóźniej 3 dni robocze przed planowanym wprowadzeniem zmian, tak aby nie zakłóciły ciągłości działania usług.
3. Dostęp do wskazanych portów i adresów jest monitorowany.
4. Niedozwolone jest:
    a. próby dostępu do innych urządzeń poza wskazanymi we wniosku – załącznik nr 1,
    b. próby przekraczania zakresu przyznanego dostępu,
    c. udostępnianie loginów i haseł osobom innym niż te, których uprawnienie dotyczy,
    d. próby ominięcia zabezpieczeń Szpitala.
5. Pracownicy Działu Informatyki mają prawo do natychmiastowego odebrania uprawnień w razie stwierdzenia rażących naruszeń bezpieczeństwa informacji.

Udzielanie i odbieranie uprawnień:

1. Strony ustalają, że właściwymi osobami ze strony Przyjmującego zlecenie do wydawania wniosków o dostęp do systemów szpitalnych będą:
    a. …….
    b. …….
2. Każda zmiana na tej liście musi być sporządzona w formie pisemnej lub dokumentem elektronicznym sygnowanym podpisem kwalifikowanym w/w osób, pod rygorem nieważności wprowadzanych zmian.
3. Przyjmujący zlecenie zobowiązuje się do przekazania informacji o cofnięciu upoważnienia do wykonywania w jego imieniu prac dla osób z listy pracowników nie później niż 3 dni robocze, a sytuacjach szczególnych w dniu cofnięcia uprawnień.
4. Przyjmujący zlecenie zobowiązuje się do przekazania listy nowych pracowników nie później niż 5 dni roboczych przed terminem wykonania pierwszych czynności serwisowych o ile umowa serwisowa nie stanowi inaczej.

Czynności serwisowe i poserwisowe

1. Przyjmujący zlecenie zobowiązuje się do każdorazowego poinformowania o zakresie prowadzonych prac i ich efektach pracowników komórki organizacyjnej, która korzysta z serwisowanego urządzenia oraz pracowników Działu Informatyki na adres mailowy techniczne.it@szpital.wroc.pl. Brak informacji o zakresie prowadzonych prac może skutkować zablokowaniem zdalnego dostępu do czasu wyjaśnienia sprawy.
2. Zabrania się podłączania do sieci Szpitalnej komputerów innych niż wykazane w umowie, chyba, że uprzednio uzyska się aprobatę pracownika Działu Informatyki. Fakt ten powinien zostać udokumentowany w protokole prac serwisowych.
3. Zabrania się wykorzystywania innych adresów IP niż wskazane przez pracowników Działu AI
4. W przypadku wymiany nośnika danych, na których mogą znajdować się dane poufne, medyczne lub osobowe, przyjmujący zlecenie jest zobowiązany do zniszczenia w/w danych w sposób trwały i potwierdzenie tego stosownym protokołem.
5. Podobnie, w przypadku rozwiązania umowy, nośniki danych na których mogą znajdować się dane poufne, medyczne lub osobowe, przyjmujący zlecenie jest zobowiązany zniszczyć danych w sposób trwały i potwierdzić ten fakt stosownym protokołem.