I N S T R U K C J A
użytkowania systemu informatycznego

w Zespole Opieki Zdrowotnej
w Łowiczu

POSTANOWIENIA OGÓLNE

§ 1. 1. Instrukcja określa warunki użytkowania systemu informatycznego i bezpieczeństwa przetwarzania informacji w tym systemie.

2. Przetwarzanie informacji w systemie informatycznym odbywa się na podstawie przepisów prawa i w zakresie określonym właściwymi przepisami oraz w zakresie niezbędnym do realizacji celów ZOZ.

3. Do przetwarzania informacji w postaci elektronicznej stosuje się przepisy wewnętrzne obowiązujące w ZOZ oraz przepisy ogólnie obowiązujące w zakresie wymiany informacji z państwowymi systemami informatycznymi.

4. Kopie informacji i wydruki, które nie podlegają obowiązkowi przechowywania lub archiwizowania powinny być niezwłocznie usuwane lub niszczone.

§ 2. Przez użyte w treści instrukcji sformułowania należy rozumieć:

1) system informatyczny – zespół środków technicznych (urządzeń), sieci (połączeń pomiędzy elementami) i oprogramowania, służący do przetwarzania informacji w postaci elektronicznej, zwany dalej systemem;
2) baza danych – uporządkowany rzeczowo zbiór danych prowadzony w formie elektronicznej wraz z oprogramowaniem;
3) Administrator Systemu Informatycznego – osoba wyznaczona przez Dyrektora, której obowiązki zostały określone w Regulaminie organizacyjnym ZOZ zwana dalej ASI;
4) przetwarzanie informacji – jakiekolwiek operacje wykonywane na informacjach;
5) użytkownik – użytkownik określony w Polityce bezpieczeństwa informacji w ZOZ, któremu nadano prawo dostępu do systemu informatycznego ZOZ w określonym celu i zakresie, działający w ramach tego prawa;
6) stacja robocza - każdy komputer lub inne urządzenie końcowe przeznaczone do bezpośredniej pracy użytkownika, w tym urządzenie mobilne;
7) dane dostępowe - login i hasło lub inne dane identyfikujące jednoznacznie użytkownika systemu.

§3. 1. Poziom zabezpieczenia informacji przetwarzanych w systemie informatycznym określa Dyrektor.

2. Dyrektor określa również poziom technicznego zabezpieczenia pomieszczeń, w których znajdują się elementy systemu, stosownie do ich ważności.

3. Wstęp do kluczowych pomieszczeń jest dozwolony tylko w obecności ASI.

OGÓLNE ZASADY EKSPLOATACJI SYSTEMU INFORMATYCZNEGO

§ 4. 1. Urządzenia oraz oprogramowanie pracujące w systemie informatycznym ZOZ muszą być zgodne ze sprzętową oraz programową konfiguracją zalecaną przez ASI i odpowiadające co najmniej minimalnym bieżącym standardom.

2. Wykorzystanie sieci bezprzewodowych powinno być ograniczone do niezbędnego minimum. Sieci takie muszą być zabezpieczone. Nie udostępnia się tych sieci osobie innej niz. użytkownik.

3. Wszystkie połączenia pomiędzy siecią zewnętrzną a systemem informatycznym ZOZ

powinny być monitorowane oraz zabezpieczone programowo. Dopuszcza się możliwość blokowania określonych zasobów sieci zewnętrznej.

§ 5. 1. Stacje robocze działające w systemie informatycznym ZOZ zabezpieczone są hasłem użytkownika oraz mają uruchomiony wygaszacz ekranu automatycznie aktywujący się po określonym czasie braku aktywności użytkownika.

2. Dostęp do baz danych chroniony jest co najmniej identyfikatorem użytkownika i hasłem użytkownika. Dostęp do określonych funkcjonalności może być chroniony dodatkowymi zabezpieczeniami.

3. Systemy informatyczne stosowane w ZOZ umożliwiają indywidualny dostęp użytkownika do określonego zakresu informacji i określonych funkcjonalności oraz rejestrują aktywność każdego użytkownika.

4. Dane dostępowe do kont użytkowników oraz funkcji administracyjnych systemu i baz danych podlegają szczególnej ochronie

§ 6. 1. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stacji roboczych powinny być ustawione w sposób uniemożliwiający tym osobom wgląd w monitor.

2. Niedopuszczalne jest umożliwienie osobie innej niż użytkownik dostępu do stacji roboczej bez uzasadnionej potrzeby oraz bez nadzoru użytkownika.

3. Współdzielona drukarka lub kopiarka nie może być pozostawiona bez kontroli użytkownika, jeśli są lub wkrótce będą drukowane na niej informacje objęte ochroną.

§ 7. 1. Dopuszczalne jest funkcjonowanie na jednej stacji roboczej więcej niż jednego konta użytkownika pod warunkiem odrębnego zabezpieczenia każdego z tych kont.

2. W wyjątkowych przypadkach, gdy wymuszają to ograniczenia sprzętowe lub programowe, jednymi danymi dostępowymi może dysponować kilku użytkowników pod warunkiem, że na podstawie danych innych niż dane logowania, można odróżnić czynności wykonane przez użytkowników.

3. Logowanie przez jednego użytkownika na kilku stacjach roboczych równocześnie z wykorzystaniem tego samego identyfikatora jest ograniczone do minimum uzasadnionego rodzajem wykonywanych zadań.

4. Wymiany informacji z zewnętrznymi systemami informatycznymi mogą dokonywać tylko wyznaczeni użytkownicy.

§ 8. 1. Dostęp do konta administratora systemu informatycznego oraz systemu operacyjnego w stacji roboczej jest zastrzeżony dla ASI lub użytkowników uprawnionych do utrzymania systemu.

2. W wyjątkowych przypadkach, gdy wymuszają to ograniczenia sprzętowe lub programowe użytkownik może korzystać z konta administratora systemu operacyjnego. Użytkownik taki nie może dokonywać czynności zastrzeżonych dla ASI.

§ 9. 1. Zabrania się testowania i podejmowania prób poznania metod zabezpieczenia systemu informatycznego ZOZ.

2. Niedopuszczalne są próby obejścia zabezpieczeń systemu informatycznego ZOZ

3. Zabronione jest korzystanie z systemu informatycznego w zakresie wykraczającym poza obowiązek zawodowy lub wynikający z umowy.

4. W przypadku korzystania z połączeń z siecią zewnętrzną użytkownik zachowuje najwyższą staranność w celu uniknięcia zagrożeń pochodzących z tej sieci.

5. Nieużywane porty powinny być dezaktywowane.

OCHRONA SPRZĘTU INFORMATYCZNEGO

§ 10. 1. Za bezpośrednią fizyczną ochronę elementów systemu informatycznego przed kradzieżą, zniszczeniem lub nieuprawnionym dostępem odpowiedzialny jest użytkownik tych elementów.

2. Pomieszczenia w których znajdują się elementy systemu informatycznego posiadają zabezpieczenia techniczne i wyposażenie stosowne do znaczenia tych elementów. Dyrektor podejmuje działania w celu podnoszenia standardu zabezpieczenia tych pomieszczeń.

3. Dostęp do pomieszczenia serwerowni oraz innych pomieszczeń kluczowych jest możliwy tylko w obecności ASI.

4. Dostęp do urządzeń zasilających i podtrzymujących zasilanie jest możliwy tylko dla upoważnionych do tego osób.

5. Użytkownicy nie mogą sami demontować ani dokonywać jakiejkolwiek zmiany elementów systemu informatycznego Czynności te są zastrzeżone dla ASI lub innych osób uprawnionych pod nadzorem ASI.

6. Elementy systemu informatycznego nie mogą być przemieszczane bez zgody ASI.

7. Zabrania się podłączania do systemu informatycznego jakichkolwiek urządzeń bez zgody ASI.

8. Zabrania się zestawiania jakichkolwiek połączeń pomiędzy elementami systemu informatycznego bez zgody ASI.

§ 11. 1. Każde urządzenie używane w systemie informatycznym ZOZ musi być oznaczone w celu jego identyfikacji.

2. Inwentaryzacji i oznaczenia sprzętu dokonuje ASI wspólnie z pracownikiem zajmującym stanowisko ds. inwentaryzacji.

§ 12. Osoba użytkująca urządzenie mobilne zawierające informacje zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania zwłaszcza poza obszarem ZOZ, w tym dodatkowo zabezpiecza hasłem dostęp do danych.

OCHRONA OPROGRAMOWANIA

§ 13. 1. Oprogramowanie używane w systemie informatycznym ZOZ jest chronione przed nieautoryzowaną modyfikacją, usunięciem lub kopiowaniem.

2. Instalacja oprogramowania może być dokonywana tylko przez ASI lub pod nadzorem ASI.

3. Użytkownicy nie mogą sami dokonywać jakichkolwiek zmian w oprogramowaniu zainstalowanym w stacji roboczej.

§ 14. 1. W systemie informatycznym ZOZ może być używane wyłącznie oprogramowanie licencjonowane przez posiadacza prawa autorskiego, używane tylko zgodnie z prawami licencji oraz zgodnie z instrukcją użytkownika.

2. ASI przechowuje dowody własności licencji, w tym oryginały dysków.

3. W systemie informatycznym ZOZ wykorzystane są narzędzia związane z bezpieczeństwem systemów tylko pochodzące od zaufanego dostawcy.

4. Każda stacja robocza musi mieć zainstalowane oprogramowanie antywirusowe. Oprogramowanie to musi być zainstalowane również na serwerach sieciowych.

5. Oprogramowanie antywirusowe uniemożliwia użytkownikowi pominięcie etapu skanowania lub dezaktywację.

6. Aktualizacje systemów operacyjnych oraz programów antywirusowych oraz aktualizacje plików identyfikujących wirusy w stacjach roboczych powinny dokonywać się automatycznie.

UDZIELANIE DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

§ 17. Udzielenie dostępu do systemu informatycznego polega na nadaniu użytkownikowi, uprawnienia do przetwarzania informacji w systemie informatycznym, poprzez nadanie identyfikatora użytkownika, hasła użytkownika oraz przydzieleniu określonych funkcjonalności w wybranych modułach bazy danych.

§ 18. Wyróżnia się następujące poziomy dostępu do systemu informatycznego:

1) poziom ogólny - dostęp do stacji roboczej oraz ewentualnie sieci zewnętrznej i poczty zakładowej bez dostępu do bazy danych,

2) poziom rozszerzony - jak w ppkt. 1), oraz do wybranych modułów i funkcjonalności w bazie danych,

3) administratora - umożliwiający nadawanie, cofanie i modyfikacje praw dostępu użytkowników do sieci informatycznej oraz modyfikację oprogramowania sieci i baz danych.

§ 19. 1. Dostęp do systemu informatycznego może być udzielony wyłącznie w zakresie nie przekraczającym minimum koniecznego do wykonywania obowiązków oraz upoważnienia do przetwarzania danych osobowych, o którym mowa w Polityce ochrony danych osobowych.

2. Dostęp jest nadawany bezterminowo na cały okres zatrudnienia lub współpracy lub na określony czas odpowiadający wykonywanemu zadaniu lub okresowi umowy.

3. Dostęp na poziomie administratora do określonej części systemu informatycznego może być nadany również użytkownikowi innemu niż ASI, który bezpośrednio odpowiada za administrowanie określonej części systemu informatycznego, jego utrzymanie bądź konserwację.

§ 20. 1. Dostęp na poziomie ogólnym jest nadawany na wniosek kierownika komórki organizacyjnej, w której użytkownik wykonuje czynności zawodowe lub Działu Spraw Pracowniczych. . Wzór wniosku określa załącznik nr 1.

2. Podstawą wystawienia wniosku o dostęp jest umowa o pracę lub inna umowa co do osoby działająca na rzecz i w imieniu ZOZ w Łowiczu na podstawie umów innych niż umowa o pracę,

3. W szczególnych sytuacjach, gdy zachodzi ryzyko dla ciągłości udzielania świadczeń opieki zdrowotnej, a nie jest możliwe złożenie wniosku o którym mowa w ust. 2 dostęp na poziomie rozszerzonym może być nadany na ustny wniosek osób o których mowa w ust. 1. Wniosek o którym mowa w ust. 2 jest sporządzany po ustaniu przyczyny.

§ 21. 1. Login użytkownika i hasło startowe nadaje ASI. Użytkownik jest zobowiązany do niezwłocznej zmiany hasła startowego.

2. Zasady określania nazwy użytkownika oraz minimalne wymogi co do długości hasła i jego elementów określa Dyrektor.

3. Użytkownik ponosi pełną odpowiedzialność za zachowanie hasła w tajemnicy.

4. Hasła nie mogą być przechowywane w formie jawnej w żadnej postaci, szczególnie w miejscach, gdzie może dojść do ich ujawnienia wobec osób postronnych.

5. Hasła nie mogą być zapisywane w opcji auto zapisywania lub auto uzupełniania hasła, nawet jeśli system to umożliwia.

6. Użytkownik natychmiast zmienia hasło, jeśli poweźmie podejrzenie, że mogło zostać ujawnione przed osobami postronnymi oraz zgłasza ten fakt ASI.

7. W przypadku utraty hasła nie skutkującej jego ujawnieniem użytkownik zgłasza się do ASI celem uzyskania hasła startowego.

§ 22. Zmiana hasła jest cyklicznie wymuszana przez bazę danych. Jeżeli baza danych nie wymusza cyklicznej zmiany hasła, użytkownik jest zobowiązany uczynić to samodzielnie, nie rzadziej niż raz w miesiącu.

§ 23. 1. osoba o której mowa w § 20 jest zobowiązana natychmiast po zakończeniu świadczenia pracy jak też po zakończeniu prowadzonej na podstawie innej umowy współpracy z osobą, która miała prawo dostępu, poinformować o tym fakcie ASI.

2. W przypadku pracowników informacja ta może odbywać się poprzez kartę obiegową zwolnienia.

3. Po uzyskaniu informacji o której mowa w ust. 1 lub 2 ASI niezwłocznie odbiera dostęp do systemu informatycznego. Odebranie dostępu może polegać na zablokowaniu użytkownika, bez usunięcia jego danych, jeżeli wymaga tego potrzeba zachowania integralność danych.

4. IOD może w uzasadnionych przypadkach zastrzec dostęp do systemu informatycznego każdemu użytkownikowi na czas niezbędny do wyjaśnienia przyczyny zastrzeżenia.

PRACA W SYSTEMIE INFORMATYCZNYM

§ 24. Użytkownicy nie mogą mieć możliwości pracy w systemie informatycznym w sposób anonimowy.

§ 25. 1. Przed przystąpieniem do pracy w systemie informatycznym w ZOZ Łowicz użytkownik powinien upewnić się, że spełnione są podstawowe warunki bezpieczeństwa wymagane przy przetwarzaniu informacji w systemie informatycznym, czy nie są podłączone inne urządzenia lub nie doszło do naruszenia zabezpieczenia pomieszczenia w czasie nieobecności użytkownika.

2. Po zakończeniu pracy w systemie informatycznym użytkownik obowiązany jest wylogować się i wyłączyć stację roboczą oraz urządzenia podtrzymujące zasilanie.

§ 26. 1. O ile system operacyjny nie wymusza automatycznie wygaszania ekranu użytkownik jest zobowiązany uruchomić wygaszanie samodzielnie.

2. W przypadku dłuższej nieobecności na stanowisku pracy użytkownik zobowiązany jest do wylogowania się programu lub z systemu.

§ 27. 1. Użytkownik przetwarza informacje w systemie informacyjnym tylko w celu i w zakresie wynikającym z powierzonych mu obowiązków.

2. W przypadku wprowadzenia błędnych danych, użytkownik sam dokonuje ich poprawienia, a jeśli wykracza to poza zakres jego uprawnień informuje o tym ASI, który dokonuje zmiany. Czynność ta nie wymaga odrębnego dokumentowania.

3. W toku pracy użytkownik jest zobowiązany obserwować pracę stacji roboczej i oprogramowania a zwłaszcza poprawność reakcji, płynność, alerty i powiadomienia i zgłaszać ASI zaobserwowane nieprawidłowości.

3. ASI jest zobowiązany do bieżącego utrzymania prawidłowego działania systemu, reagowania na zgłoszenia użytkowników, informowania użytkowników o planowanych działaniach mających wpływ na pracę użytkownika, przeszkolenia użytkownika w zakresie udzielanego mu dostępu do systemu.

4. Kierownik komórki organizacyjnej zgłasza ASI potrzeby programowe i sprzętowe, określa i weryfikuje zakres uprawnień przyznanych podległemu użytkownikowi, nadzoruje korzystanie przez podległych mu użytkowników z system, identyfikuje zagrożenia w obrębie podległej komórki.

KORESPONDENCJA DROGA ELEKTRONICZNĄ

§ 28. 1. Korespondencja drogą elektroniczną jest prowadzona przy użyciu poczty zakładowej.

2. Wysyłanie korespondencji służbowej z prywatnego adresu e-mail jest dopuszczalne tylko w sytuacjach awaryjnych. Należy następnie usunąć wszelkie informacje w tym również z kosza.

§ 29. 1. W korespondencji drogą elektroniczną dane osobowe lub inne ważne informacje powinny być przesyłane w załącznikach zabezpieczonych hasłem, które nie powinno być przekazywane w treści tej korespondencji.

2. Do korespondencji prowadzonej systematycznie z zaufanymi podmiotami zewnętrznymi nie jest konieczne każdorazowe ustanawianie odrębnego hasła.

2. Korespondencja elektroniczna, w tym załączniki muszą być tytułowane zgodnie ze swoją treścią.

§ 30. 1. Zabronione jest otwieranie załączników do wiadomości pochodzących od nieznanego nadawcy, lub z treści których nie wynika aby to była korespondencja służbowa. Wiadomości te powinny być niezwłocznie usuwane również z kosza.

2. Zabronione jest odpowiadanie na wiadomości generowane automatycznie, nie zamówione oferty, oraz wiadomości potencjalnie szkodliwe.

3. Zabronione jest przechowywanie w poczcie wiadomości zawierających zbiory danych osobowych lub zbiory informacji źródłowych.

UŻYTKOWANIE URZĄDZEŃ MOBLINYCH

§ 31. Postanowienia instrukcji stosuje się do urządzeń mobilnych. z zastrzeżeniem zmian ujętych w niniejszym rozdziale.

§ 32. 1. Urządzenie mobilne jest udostępniane użytkownikowi na wniosek kierownika komórki organizacyjnej.

2. Użytkownicy mogą z własnej woli, do celów zawodowych, korzystać z własnych telefonów komórkowych zachowując zasady bezpieczeństwa określone w tym rozdziale.

3. Rejestr użytkowników urządzeń mobilnych jest prowadzony w ramach ewidencji majątkowej.

4. Urządzenia mobilne nie mogą być użyczane przez użytkownika innej osobie.

5. Użytkownik ponosi odpowiedzialność za poufność informacji przekazywanych za pośrednictwem urządzenia moblilnego.

6. W przypadku zwracania urządzenia użytkownik usuwa z niego wszystkie dane, chyba że Dyrektor postanowi inaczej.

§ 33. 1. Użytkownik ponosi odpowiedzialności za fizyczne bezpieczeństwo urządzenia oraz nienaruszalność zawartych w nim danych.

2. Połączenia Wi-Fi i Bluetooth mogą być włączone tylko na czas korzystania z nich. Nie należy nawiązywać połączeń z nieznanymi sieciami bezprzewodowymi.

§ 34. Zabronione jest przechowywanie w urządzeniach mobilnych zbiorów danych, za wyjątkiem danych kontaktowych do osób i podmiotów współpracujących oraz informacji źródłowych.

§ 35. Użytkownik może samodzielnie dokonywać aktualizacji oprogramowania systemowego. Zabronione jest instalowanie w urządzeniu innych aplikacji.

§ 36. Dozwolone jest przemieszczania urządzeń mobilnych poza miejsce pracy oraz korzystanie z nich poza czasem pracy.

DODATKOWE WYMOGI DOTYCZĄCE PRACY ZDALNEJ

§ 37. 1. Wykonywanie przez użytkownika pracy zdalnej jest dozwolone tylko za zgodą Dyrektora co do zasadności oraz zgodą ASI co do warunków bezpieczeństwa i musi się odbywać przy wsparciu i pod nadzorem ASI.

2. Praca zdalna w systemie jest dopuszczalna wyłącznie za pośrednictwem połączeń VPN. Ewidencja użytkowników VPN jest prowadzona w systemie. Połączenie VPN jest chronione co najmniej loginem i hasłem.

3. Praca bez dostępu do bazy danych może się odbywać bezpośrednio w stacji roboczej użytkownika.

4. Użytkownikom zabrania się samodzielnego uruchamiania programów i aplikacji, które nawiązują połączenia VPN.

§ 38. Administrator Systemu Informatycznego może używać VPN do nadzorowania systemu informatycznego po godzinach pracy z dogodnej dla siebie lokalizacji, pod warunkiem, że logowanie nie odbędzie się z publicznych punktów dostępu do sieci Internet.

§ 39. 1. Dopuszcza się stały dostęp VPN dla komórek organizacyjnych ulokowanych poza główną siedzibą ZOZ.

2. Dopuszcza się za wiedzą ASI dostęp VPN dostawcy kluczowych usług informatycznych w celu naprawy, konserwacji lub modernizacji systemu.

§ 40. 1. W ramach pracy zdalnej dopuszczalne jest korzystanie przez użytkownika z prywatnej stacji roboczej.

2. Prawa własności intelektualnej w takim przypadku należą do ZOZ.

3. Stacja robocza musi mieć zainstalowane oprogramowanie antywirusowe i zaktualizowany system operacyjny.

4. Użytkownik jest zobowiązany chronić dostęp do stacji roboczej co najmniej poprzez hasło systemu operacyjnego oraz chronić przetwarzane dane przed dostępem osób postronnych tak jak na stanowisku pracy

5. Niedopuszczalne jest tworzenie kopii informacji w prywatnej stacji roboczej a jeżeli wynika to z charakteru pracy, dane takie należy usunąć niezwłocznie, w tym również z kosza.

6. Podczas połączenia z systemem informatycznym ZOZ nie jest dopuszczalne korzystanie z innych połączeń internetowych.

ELEKTRONICZNE NOŚNIKI DANYCH

§ 41. 1. Postanowień rozdziału nie stosuje się do przypadków, kiedy dany proces przetwarzania lub obowiązek prawny wymaga zapisywania informacji na elektronicznych nośnikach danych.

2. Czynności, o której mowa w ust. 1 mogą dokonywać tylko wyznaczeni użytkownicy.

§ 42. 1. Elektroniczne nośniki danych, za wyjątkiem określonym w § 41. 1. są ewidencjonowane przez ASI.

2. Ogranicza się, do wyjątków za zgodą Dyrektora, liczbę stacji roboczych, które dają użytkownikowi możliwość zapisu lub odczytania elektronicznych nośników danych. ASI prowadzi ewidencję stacji roboczych dających taką możliwość.

3. Za elektroniczny nośnik danych oraz bezpieczeństwo zapisanych na nim informacji odpowiada użytkownik nośnika.

4. Elektroniczne nośniki danych powinny być po zakończeniu pracy przechowywane w sposób zapewniający bezpieczeństwo zapisanych na nim informacji przed utratą, modyfikacją oraz nieuprawnionym dostępem.

5. Przemieszczanie elektronicznych nośników danych poza teren ZOZ jest zabronione. O ile zachodzi taka konieczność informacje na nośnikach muszą być zaszyfrowane i zabezpieczone co najmniej hasłem.

§ 43. 1. Podłączanie przez użytkownika do systemu informatycznego jakichkolwiek elektronicznych nośników danych pochodzących z zewnątrz ZOZ jest zabronione. Jeżeli jest to konieczne, czynności ta może byś dokonana wyłącznie po uprzednim sprawdzeniu nośnika przez ASI.

2. Użytkownicy nie mogą kopiować oprogramowania, ani informacji z systemu na elektroniczne nośniki danych, a gdy wymaga tego określony proces przetwarzania, dane powinny być zaszyfrowane co najmniej przy użyciu powszechnie dostępnego oprogramowania.

§ 44 . 1. Informacje źródłowe nie mogą być przechowywane na jednym elektronicznym nośniku danych.

2. W przypadku przechowywania źródłowych informacji na elektronicznych nośnikach danych przez dłuższy okres czasu należy co najmniej jeden raz w roku kontrolować jakość zapisu oraz uwzględnić utratę własności nośnika oraz późniejszą dostępność formatu zapisu.

3. Do elektronicznych nośników danych używanych do przechowywania informacji w celach archiwalnych stosuje się dodatkowo przepisy archiwalne.

§ 45. Przeznaczone do likwidacji elektroniczne nośniki danych należy przekazać ASI, który dokonuje nieodwracalnego mechanicznego zniszczenia.

POSTEPOWANIE Z INCYDENTAMI I SYTUACJAMI AWARYJNYMI

§ 61. W przypadku ujawnienia zakłócenia w pracy systemu informatycznego spowodowanego nieprawidłowym działaniem oprogramowania, sprzętu lub użytkownika podejmuje się działania określone w niniejszym rozdziale.

§ 62. 1. W przypadku nieprawidłowej pracy systemu użytkownik może samodzielnie jednokrotnie zamknąć i ponownie uruchomić oprogramowanie lub stację roboczą w celu wymuszenia automatycznej naprawy. Jeżeli działanie to nie przyniosło oczekiwanego skutku użytkownik zaprzestaje pracy w systemie i powiadamia ASI.

2. Jeżeli zachodzi uzasadnione podejrzenie, że nieprawidłowość mogło spowodować złośliwe oprogramowanie, należy niezwłocznie wyłączyć stację roboczą, odłączyć ją od sieci oraz powiadomić ASI.

3. W przypadkach określonych w ust. 1 i 2 użytkownik przekazuje ASI również informację o ostatnio wykonywanych w systemie działaniach oraz stwierdzonych objawach zdarzenia.

4. Użytkownik nie może podejmować żadnych działań, które by mogły utrudnić lub uniemożliwić przywrócenie prawidłowego stanu systemu ani zacierać dowodów.

§ 64. Użytkownik, który ujawnił niezgodne z instrukcją lub innymi przepisami wewnętrznymi korzystanie z systemu informatycznego jest zobowiazany zgłosić ten fakt przełożonemu.

§ 65. Za niezgodne z instrukcją lub innymi przepisami wewnętrznymi korzystanie z systemu informatycznego użytkownik ponosi odpowiedzialnosc porządkową lub jesli nie jest pracownikiem, inną odpowiedzialność określoną w umowie.

DOPUSZCZANIE SPRZETU

§ 50. 1. Autoryzacji podlegają wszystkie nowe modele urządzeń mające być użyte w systemie.

2. Autoryzacji podlega również sprzęt nie będący własnością ZOZ, służący do przetwarzania danych związanych z działalnością ZOZ.

§ 51. Autoryzacja obejmuje sprawdzenie, czy: urządzenie posiada certyfikaty i homologacje wymagane na terenie kraju, spełnia wymagania techniczne dotyczące podłączenia go do systemu, spełnia wymagania bezpieczeństwa oraz Polityki Bezpieczeństwa Informacji, posiada funkcjonalność umożliwiającą ustalenie zakresu dostępu uzytkowników, nie spowoduje zakłoceń w pracy systemu.

ZARZADZANIE ZMIANĄ

§ 52. 1. Wprowadzanie i nadzorowanie zmian wprowadzanych do systemów informatycznych, zmiana konfiguracji, funkcjonalności, kluczowych komponentów systemu¬ informatycznego może byc wykonywane wyłacznie przez ASI lub za jego wiedzą przez zaufanego dostawcę usług.

2. Wprowadzenie zmian jest dopuszczalne wyłącznie po wykluczeniu negatywnego wpływu zmiany na system.

3. Nie dopuszcza się zmian w oprogramowaniu, które nie są podyktowane względami bezpieczeństwa bądź istotną modyfikacją funkcjonalności.

4. Wprowadzanie zmian do systemu informatycznego powinno być realizowane w sposób umożliwiający przywrócenie stanu wyjściowego przed zmianą

5. Zmianą jest również podniesienia aplikacji lub systemu do wyższej wersji.

§ 53. 1. Wprowadzanie zmian powinno być poprzedzone próbą na maszynie testowej, na której odtworzono środowisko pracy stacji docelowej w niezbędnym zakresie.

2. Funkcję stacji testowej może pełnić dowolna dostępna stacja robocza, po zapewnieniu bezpiecznego usunięcia z niej informacji i oprogramowania po zrealizowanym teście, pod warunkiem uprzedniego zabezpieczenia przechowywanych na niej danych.

3. Jeżeli wymagają tego względy bezpieczeństwa nalezy przed przeprowadzenierm testu, wykonać obrazu systemu wraz z niezbędnymi aplikacjami, celem pełnego odtworzenia środowiska pracy.

§ 54. 1. Od przeprowadzenia testu można odstąpić jedynie w przypadku, gdy ASI dysponuje już wiedzą, że wprowadzenie zmiany nie pociąga za sobą zagrożeń dla systemu, lub że wprowadzenie zmiany jest niezbędne ze względów bezpieczeństwa, a ewentualne zakłócenia w funkcjonowaniu systemu są zidentyfikowane i zagrożenia wynikające z nich są mniejsze niż koszty zaniechania wprowadzenia zmiany.

.

§ 55. 1. W przypadku stwierdzenia niekorzystnego wpływu zmian na funkcjonowanie systemu, ASI niezwłocznie podejmuje działania w celu wyeliminowania bądź zminimalizowania negatywnych skutków zmiany.

2. W przypadku, gdy zmiana skutkuje odmienną niż dotychczasowa konfiguracją stacji roboczej, ASI niezwłocznie przekazuje informacje niezbędne dla aktualizacji dokumentacji stacji roboczej oraz przekazuje niezbędne informacje uzytkownikowi.

3. W przypadku, gdy zmiana skutkuje ingerencją w prawa dostępu do informacji, ASI uzgadnia możliwość jej wprowadzenia z właścicielami tych zasobów.

§ 56. 1. Jeżeli wprowadzenie zmiany wiąże się z opracowaniem przez firmę zewnętrzną dedykowanego oprogramowania, ASI zgodnie z odpowiednimi zapisami umowy wiążącej strony nadzoruje proces tworzenia oprogramowania.

2. Nadzór nad pracami ma zapewnić, że zostały podjęte wszelkie niezbędne środki przewidziane umową, mające wpływ na zachowanie poufności w trakcie realizacji umowy, w szczególności w zakresie postępowania z informacjami istotnymi dla bezpieczeństwa organizacji.

PRZEGLĄD I KONSERWACJA SYSTEMU INFORMATYCZNEGO

§ 57. 1. ASI odpowiada za określanie kierunków rozwoju systemu informatycznego, identyfikowanie nowych zagrożeń dla bezpieczeństwa systemu informatycznego i podejmowanie działań zaradczych oraz monitoruje zewnętrzne źródła informacji pod kątem nowych zagrożeń realności ich zaistnienia w systemie i ich krytyczności.

2. ASI monitoruje na bieżąco działanie systemu, aplikacji, stacji roboczych oraz użytkowników pod kątem niestandardowych zachowań

§ 58. 1. Wszystkie zmiany w obrębie systemu informatycznego powinny być udokumentowane w kolejności ich dokonania.

2. System informatyczny prowadzi zapis wszystkich znaczących zdarzeń systemowych mających wpływ na bezpieczeństwo przetwarzanych w nich danych osobowych.

3. ASI prowadzi w systemie ewidencję urządzeń wraz z opisem ich konfiguracji i oprogramowania.

§ 59. 1. Naprawy i przeglądy urządzeń i oprogramowania mogą być dokonywane tylko

przez ASI.

2. Jeżeli naprawy lub przeglądy wymagają specjalistycznej wiedzy lub uprawnień powinny odbywać się pod nadzorem ASI lub osoby użytkującej urządzenie, a w przypadku naprawy urządzenia poza ZOZ należy usunąć z urządzenia informacje.

§ 60. 1. Ewidencja użytkowników jest prowadzona w systemie informatycznym.

2. Raz w roku ASI wspólnie z IOD dokonuje weryfikacji uprawnień poszczególnych użytkowników systemu.

§ 61. 1. Raz w roku ASI przeprowadza weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich stacjach roboczych pod kątem spełnienia wymogów bezpieczeństwa.

2. ASI raz na kwartał powinien przeprowadzać weryfikację usług sieciowych dostępnych w systemach informatycznych oraz blokować usługi niewykorzystywane jak również uaktualniać systemy operacyjne i aplikacje.

Łowicz dnia.....

Administrator

Systemu Informatycznego

Proszę o nadanie prawa dostępu do bazy danych w zakresie niżej zaznaczonych modułów dla (imię i nazwisko) ….....

….....

.....

..ewentualnie dane dodatkowe jeśli system wymaga (komórka org. zawód, nr uprawnień).

*-zakreślić wybrane lub dopisać.

ESCULAP

ANE	IPO	OFR	PBW	PGP	PMP	PTK	STAT	….....
APT	IPP	ONEO	PCH	PGPZ	POEN	REJ	TS	….....
ATS	LAB	OPE	PCHU	PHEM	POR	REJ2	USG1	….....
ATS	MAG	OPG	PEN2	PIMM	POZ	REJL	USG2	….....
BAKT	NPL	OWEW	PEND	PKAR	PREH	REJP	ZRD	.
BLOK	OAIT	PANA	PFIZ	PKOA	PRTG	RTG	ZRH	
IPG	OCH	PBIO	PGER	PLU	PSE	RTG2	….....	

SIMPLE

analizy	kokpit zaopatrzeniowca	….....
produkcja	programowanie	.
personel	pulpit administratora	….....
majątek trwały	zarządz. operacyjne majątkiem	….....
oferowanie	rekompensata	
budżetowanie	zarządz. bezp. danych	

Pieczątka i podpis

kierownika komórki organizacyjnej lub
Działu Spraw Pracowniczych