Załącznik nr 1 do uchwały nr 156/VIII/2018 Okręgowej Rady Lekarskiej Beskidzkiej Izby Lekarskiej z dnia 3 lipca 2018 roku w sprawie zmiany uchwały nr 281/VII/2017 Okręgowej Rady Lekarskiej Beskidzkiej Izby Lekarskiej z dnia 30 czerwca 2017 roku w sprawie instrukcji zarządzania systemem informatycznym Beskidzkiej Izby Lekarskiej.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Beskidzka Izba Lekarska
ul. Krasińskiego 28
43-300 Bielsko-Biała

Spis treści

I. Definicje i skróty stosowane w dokumencie.

1. **Polityka** - Polityka Bezpieczeństwa w Beskidzkiej Izbie Lekarskiej.
2. **Izba –** Beskidzka Izba Lekarska.
3. **Polityka –** Polityka Bezpieczeństwa.
4. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
5. **System informatyczny** - sprzęt i programy komputerowe którego funkcją jest przetwarzanie danych osobowych.
6. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem Ustawy, nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
7. **Administrator danych osobowych (ADO)** – Beskidzka Izba Lekarska reprezentowana przez Prezesa Okręgowej Rady Lekarskiej**,** zwany dalej ADO.
8. **Inspektor ochrony danych (IOD)** - osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie, zwany dalej IOD.
9. **Administrator Systemów Informatycznych (ASI)** - osoba wyznaczona przez Administratora odpowiedzialna za wdrażanie technicznych zabezpieczeń systemów informatycznych, ich sprawność i konserwację oraz ochronę w przetwarzanych zbiorach danych osobowych, zwana dalej ASI.
10. **Użytkownik** - osoba posiadająca upoważnienie wydane przez Administratora lub wyznaczoną przez niego osobę uprawnioną, dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
11. **Przełożony** - osoba pełniąca funkcję kierownika komórki organizacyjnej, będąca przełożonym użytkownika.
12. **Opiekun** - kierownik komórki organizacyjnej lub inna wyznaczona przez ADO osoba odpowiedzialna za dany zasób danych osobowych, zgodnie z zakresem pełnionych obowiązków.
13. **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.
14. **Zasady** - Zasady ochrony danych osobowych – szczegółowe wytyczne stanowiące załącznik do Polityki.
15. **Instrukcja** - Instrukcja zarządzania systemem informatycznym.

16. **Ustawa –** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).
17. **Rozporządzenie -** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
18. **Oświadczenie** – Druk Oświadczenie użytkownika, stanowiący załącznik do Polityki.

II. Procedura nadawania uprawnień do przetwarzania danych osobowych w systemach informatycznych.

1. Nadawanie uprawnień do korzystania z systemu informatycznego odbywa się zgodnie z zasadą wiedzy koniecznej i zasadą minimalnych uprawnień.
2. Użytkownik powinien mieć dostęp tylko do tych informacji, które są mu potrzebne do realizacji zadań. Dostęp do innych danych powinien być zabroniony.
3. Za określenie ról Użytkowników odpowiedzialni są Opiekunowie, którzy definiują typy użytkowników w oparciu o zakresy obowiązków podległych sobie pracowników.
4. Opisy ról powinny być zaakceptowane przez ASI lub IOD w celu sprawdzenia, czy wymagane uprawnienia nie stanowią zagrożenia dla przetwarzanych danych w systemie informatycznym.
5. Z pisemnym wnioskiem (załącznik 2 do Instrukcji) o nadanie uprawnień do systemu informatycznego występuje bezpośredni Przełożony do ASI. ASI określa zakres nadanych Użytkownikowi uprawnień na Wniosku.
6. W przypadku wnioskowania o nadanie uprawnień dostępu do systemu informatycznego dla podmiotu zewnętrznego występuje pracownik koordynujący jego działanie.
7. IOD może określić rodzaje informacji do których nadanie uprawnień powinno być z nim konsultowane.
8. W przypadku zastosowania systemu ról do zarządzania dostępem do informacji osoba wnioskująca podaje rolę jaka powinna być nadana użytkownikowi, z ewentualnym określeniem opcjonalnych uprawnień.
9. Nadawanie uprawnień do informacji wrażliwych jest konsultowane z IOD, a potwierdzanie nadanych uprawnień jest wykonywane przez ASI na Wniosku.
10. Użytkownik potwierdza nadane uprawnienia na Wniosku.
11. Wniosek przechowywany jest przez ASI przez okres zatrudnienia użytkownika lub jego współpracy z przedsiębiorstwem, a także przez okres przechowywania dokumentów archiwalnych.
12. Informacja o przypisanym użytkownikowi identyfikatorze przechowywana przez ASI i udostępniany jest IOD.
13. Identyfikator powinien być unikalny dla każdego użytkownika, nie należy stosować identyfikatora należącego do innej osoby nie korzystającej już z systemu informatycznego.
14. O nadaniu Użytkownikowi uprawnień administracyjnych do systemu informatycznego powinien być poinformowany IOD.
15. Administrator systemu informatycznego jest odpowiedzialny za cofnięcie uprawnień po upływie wyznaczonego okresu. Istnieje możliwość nadania użytkownikowi tymczasowych

uprawnień do korzystania z określonych zasobów. Proces nadawania uprawnień tymczasowych jest taki sam jak dla normalnych Użytkowników. Ewentualne przedłużenie okresu, w jakim użytkownik posiada uprawnienia, może nastąpić na wniosek osoby występującej o nadanie uprawnień lub osoby ją zastępującej.

16. W przypadku zmiany obowiązków służbowych lub zadań użytkownika, w szczególności zmiany komórki organizacyjnej, w której dana osoba pracuje lub na rzecz której wykonuje zadania, może okazać się konieczna zmiana uprawnień w systemie informatycznym. Jeżeli jest to związane wyłącznie z nadaniem dodatkowych uprawnień, to mogą być one nadane przez ASI na wniosek Przełożonego.

17. Zmiana uprawnień użytkownika w systemie informatycznym w którym zaimplementowano mechanizm ról, wiąże się z odebraniem starej roli użytkownikowi i nadaniem nowej. Proces rozszerzania lub modyfikacji uprawnień w uzasadnionych przypadkach podlega akceptacji IOD w szczególności, jeżeli uprawnienia wiążą się z dostępem do informacji wrażliwych.

18. Całkowite odebranie uprawnień użytkownikowi związane jest z zakończeniem jego pracy w Izbie lub współpracy z nim. Uprawnienia są odbierane przez ASI na wniosek Przełożonego Użytkownika. W szczególnych przypadkach uprawnienia mogą być odebrane na wniosek IOD jako jego reakcja na poważny incydent mający wpływ na bezpieczeństwo przetwarzanych informacji. Użytkownikowi powinny być odebrane wszystkie posiadane przez niego uprawnienia w zakresie informacji przetwarzanych w systemie informatycznym, a możliwość korzystania z identyfikatora posiadanego przez użytkownika powinna zostać zablokowana.

III. Metody i środki uwierzytelniania w systemie informatycznym.

1. Zabezpieczenie zasobów informacyjnych przed dostępem do nich osób niepowołanych wymaga podjęcia działań związanych zarówno z bezpieczeństwem fizycznym pomieszczeń, w którym znajdują się komponenty informatyczne, jak i z ochroną dostępu logicznego do samego systemu informatycznego.

2. Pomieszczenia, w którym znajduje się sprzęt informatyczny, powinny być zabezpieczony przed dostępem osób nieupoważnionych poprzez instalację odpowiednich zamków. Osoby nie będące pracownikami mogą przebywać w pomieszczeniu wyłącznie w asyście upoważnionego pracownika.

3. Użytkownicy systemu informatycznego są odpowiedzialni za zabezpieczenie powierzonych im informacji przed dostępem osób nieupoważnionych. Dotyczy wszelkich dokumentów w postaci papierowej, które podobnie jak przenośne nośniki danych (pendriv-y, CD-ROM-y), powinny być przechowywane w zamykanych szafach. Zaleca się, aby na stacjach roboczych użytkowników były otwarte tylko te aplikacje, które są przez nich w danej chwili użytkowane.

4. System informatyczny wyposażony jest w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych.

5. Identyfikator wraz z jego imieniem i nazwiskiem wpisuje się do ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzonej przez Kierownika Biura BIL.

6. Identyfikator nie powinien być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie powinien być przydzielany innej osobie.

7. Użytkownik, który utracił uprawnienia dostępu do danych osobowych, należy bezzwłocznie wyrejestrować z Systemu informatycznego, w którym są one przetwarzane, unieważnić jego hasło oraz podjąć stosowne działania w celu zapobieżenia dalszemu dostępowi tego Użytkownika do danych osobowych.

8. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w te dane.

9. Niepowtarzalny login oraz hasło jednorazowe są przydzielone użytkownikowi przez ASI po nadaniu uprawnień do przetwarzania danych osobowych.

10. Hasło jednorazowe do jest przekazane Użytkownikowi przez ASI w formie pisemnej.

11. Bezpośredni dostęp do danych Użytkownik uzyskuje po podaniu loginu i właściwego hasła.

12. Bezpieczne korzystanie z haseł wymaga implementacji podstawowych, opisanych poniżej zasad:

    a. hasło jest znane tylko użytkownikowi, któremu zostało przydzielone
    b. hasło nie jest udostępniane innym osobom (możliwe są wyjątki, np. wspólne hasła administracyjne, ale nawet w takich przypadkach zaleca się, aby każdy administrator dysponował oddzielnym kontem administracyjnym i oddzielnym hasłem)
    c. hasło jest przechowywane w bezpiecznym miejscu – najlepiej, jeżeli jest zapamiętane
    d. hasła administracyjne są przechowywane w bezpiecznym miejscu dostępnym tylko osobom upoważnionym
    e. w przypadku podejrzenia hasła użytkownik natychmiast zmienia hasło i musi poinformować o tym ABI, który podejmuje kroki w celu wyjaśnienia czy hasło to nie zostało wykorzystane do nieuprawnionego dostępu do systemu informatycznego i czy na skutek tego nie zaistniały szkody
    f. minimalna długość hasła powinna wynosić 8 znaków
    g. hasło nie powinno być pojedynczym wyrazem
    h. hasło nie powinno bezpośrednio nawiązywać do jego użytkownika (na przykład nie powinno być numerem jego telefonu, datą urodzenia, adresem itp.)
    i. hasło powinno zawierać wielkie i małe litery, cyfry lub znaki specjalne (na przykład #, *, &), o ile jest to technicznie możliwe ze względu na aplikację wykorzystującą mechanizm haseł
    j. w przypadku nadawania użytkownikowi po raz pierwszy uprawnień lub kasowania hasła ASI powinien wygenerować hasło tymczasowe, które powinno być zmienione przy pierwszym dostępie do aplikacji
    k. hasła powinny być okresowo zmieniane przez użytkowników – wymaga się zmiany co 90 dni w przypadku haseł chroniących do informacji zwykłych (możliwych do

sklasyfikowania jako informacje wewnętrzne) oraz co 30 dni w przypadku haseł chroniących dostęp do informacji wrażliwych

l. zabronione jest używanie polskich znaków diaktrycznych (ą, ś, ć, ń, ż, ź, ę, ł, ó) w hasłach,
m. zabronione jest zapisywanie hasła w pobliżu miejsca pracy lub w postaci zapisu elektronicznego w pliku w komputerze
n. przy zmianie hasła użytkownik nie powinien wprowadzać jako nowego hasła jednego z kilku poprzednich używanych (zaleca się, aby nowe hasło było różne od 4 ostatnich haseł)
o. aplikacje sprawdzające tożsamość przy pomocy hasła nie powinny wyświetlać go na ekranie monitora podczas wprowadzania przez użytkownika
p. wprowadzenie hasła nie powinno być zautomatyzowane na przykład poprzez przypisanie go klawiszowi funkcyjnemu
q. w przypadku kilkukrotnego błędnego wprowadzenia hasła (3 razy) konto użytkownika powinno ulec zablokowaniu, może być ono odblokowane przez ASI, z powiadomieniem IOD.

13. Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez ASI, gdy uzyskują lub tracą prawo dostępu do systemu.
14. Login po wyrejestrowaniu użytkownika zostaje zablokowany przez ASI.
15. Login po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.
16. Hasła do serwerów, aktywnych urządzeń sieci i istotnych programów konfiguracyjnych Administrator Systemu umieszcza w zapieczętowanych kopertach i składa w obecności IOD w metalowej szafie zamykanej na klucz. Otwarcie koperty może nastąpić w przypadku:

    a. zamiaru zniszczenia nieaktualnych haseł przez Administratora Systemu,
    b. zaistnienia konieczności zapoznania się z jej zawartością spowodowanej rezygnacją z pracy, pozbawieniem uprawnień lub śmiercią Administratora Systemu; uprawnienie w tym zakresie posiada Administrator Danych Osobowych.

IV. Procedury pracy w systemie informatycznym.

1. W celu rozpoczęcia pracy w systemie informatycznym Użytkownik obowiązany jest do wprowadzenia loginu i hasła dostępu do systemu informatycznego.
2. Podczas pierwszego uwierzytelniania w systemie informatycznym Użytkownik ma obowiązek zmiany hasła.
3. Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż raz na kwartał.
4. Zabrania się wpisywania hasła lub jego zmiany w obecności innych osób.
5. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

6. W przypadku zagubienia hasła użytkownik musi skontaktować się z ASI w celu uzyskania nowego hasła.
7. Użytkownikowi wolno używać tylko zainstalowanego oprogramowania, wyłącznie zgodnie z instrukcją obsługi, warunkami licencji i bezpieczeństwa przetwarzania danych.
8. W celu zawieszenia/wstrzymania pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wylogowania się z systemu operacyjnego.
9. W przypadku komputerów PC po wylogowaniu się z systemu operacyjnego użytkownik blokuje pulpit uniemożliwiając dostęp do danych osobom niepowołanym.
10. W celu ponownego przystąpienia do pracy w systemie użytkownik loguje się na swoje konto w komputerze i rozpoczyna pracę w systemie informatycznym zgodnie z procedurą rozpoczęcia pracy w systemie informatycznym.
11. Zabrania się pozostawiania stanowiska komputerowego z uruchomionym systemem bez kontroli pracującego na nim użytkownika.
12. Na komputerach, na których przetwarzane są dane osobowe wygaszacz ekranu zabezpieczony hasłem jest ustawiony na 10 min., na pozostałych 15 min.
13. W przypadku podejrzenia naruszenia/naruszenia bezpieczeństwa systemu informatycznego Użytkownik zgłasza incydent zgodnie z trybem postępowania opisanym w Instrukcji postępowania stanowiącej załącznik nr Z-08 do Polityki.
14. W celu zakończenia pracy w systemie informatycznym użytkownik wyrejestrowuje się z programu służącego do obsługi danych osobowych.
15. Użytkownik zamyka system operacyjny i wyłącza komputer.

V. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach.
2. W szczególnych przypadkach, za zgodą IOD, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych niepodłączonych do sieci komputerowej Izby.
3. Dane w postaci elektronicznej przetwarzane w systemie informatycznym zapisane na nośnikach informacji (np. dyskietkach, płytkach, dyskach magnetooptycznych, czy dyskach twardych) są własnością Izby.
4. Kopie zapasowe baz danych powinny być wykonywane po każdym zakończonym dniu pracy.

5. Co najmniej raz na dwa tygodnie wykonywane są kopie pełne - czyli kopia programu i baz danych. W pozostałych dniach stosuje się kopie przyrostowe, czyli zawierających zapis jedynie tych informacji, które podczas ostatniej doby uległy zmianie.
6. Kopie pełne wykonywane są również przy zmianie wersji oprogramowania.
7. Kopie danych sporządza się na:
   a. dysk przenośny
   b. pendrive
   c. serwer
   d. dysk sieciowy Boxx
8. Każdy nośnik danych CD, DVD zawierający kopię zapasową powinien być opisany:
   a. nr nośnika,
   b. data stworzenia kopii,
   c. rodzaj przechowywanych danych,
   d. okresy z jakiego pochodzą dane,
   e. nr wersji bazy danych i aplikacji.
9. Kopie danych mogą być wykonywane:
   a. automatycznie za pomocą aplikacji archiwizujących dane,
   b. ręcznie po kontrolą osoby uprawnionej.
10. Pełne kopie bezpieczeństwa należy wykonywać dla systemu operacyjnego serwera.
11. Archiwizacja programu FINN 7 SQL jest wykonywana codziennie po zakończonej pracy na dysk przenośny. Na koniec tygodnia kopię dodatkowo wykonuje się na pendrive.
12. Główny księgowy, codziennie na koniec dnia archiwizuje dokumenty księgowe na serwer.
13. Kopia programów księgowo-kadrowych wykonywana jest raz w tygodniu na serwer.
14. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
15. Jeżeli dane osobowe za zgodą ABI przetwarzane są lokalnie na stanowiskach komputerowych, obowiązek wykonania kopii bezpieczeństwa aplikacji oraz codziennego wykonywania kopii bezpieczeństwa bazy danych oraz ich bezpiecznego przechowywania, spoczywa bezpośrednio na użytkowniku danej aplikacji.
16. Archiwizacja plików użytkownika jest wykonywana przez użytkownika poprzez przeniesienie na dysk sieciowy Boxx.
17. Fakt wykonania kopii bezpieczeństwa administrator systemu odnotowuje w rejestrze tworzenia kopii bezpieczeństwa.

VI. Tworzenie archiwum kopii zapasowych.

1. Tworzenie archiwum polega na usunięciu danych z bieżących baz danych i przeniesieniu ich:
    a. do specjalnie utworzonych baz archiwalnych,
    b. do wyznaczonych miejsc ich gromadzenia na dysku,
    c. na informatyczne nośniki danych.
2. Archiwa gromadzą dane, które zostały wytworzone powyżej 12 miesięcy.
3. Archiwa tworzone są na płytach dvd, dyskach magnetycznych i pendrive.
4. Każdy zbiór danych archiwizowanych powinien mieć założoną „Kartę opisową zbioru danych archiwalnych" - druk Z-11 stanowiący załącznik do Dokumentacji.
5. Każde archiwum utworzone na zasobach dyskowy powinien być odpowiednio uporządkowany w katalogach i opisany w Rejestrze archiwum.
6. Każdy nośnik danych archiwalnych powinien być opisany:
    a. nr nośnika,
    b. data stworzenia archiwum,
    c. rodzaj przechowywanych danych,
    d. okresy z jakiego pochodzą dane,
    e. nr wersji bazy danych i aplikacji.
7. Każda operacja stworzenia archiwum powinna być odnotowana w rejestrze archiwum.

VII. Zasady przechowywania kopii zapasowych oraz elektronicznych nośników informacji zawierających dane osobowe.

1. Tworzone archiwa na nośnikach danych powinny być sprawdzane okresowo co 6 miesięcy czy ich zawartość jest możliwa odczytania i wykorzystania. Czynności te powinny być odnotowany w Rejestrze archiwum.
2. W przypadku niemożności odtworzenia jednej z dwóch istniejących kopii archiwalnych należy sporządzić drugą kopię wykorzystując do tego istniejące archiwum. Operacja ta powinna być odnotowana w Rejestrze archiwum.
3. Kopie danych zawierające rejestr lekarzy przechowuje się stosownie do aktualnie obowiązujących przepisów.
4. Po okresie przechowywania dane archiwalne oraz dane z pełnych kopii zgromadzone na pendrive i dysku przenośnym są usuwane a nośniki przekazuje się do bieżącej eksploatacji. Operacja ta powinna być odnotowana w Rejestrze archiwum.
5. Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych.
6. Po zakończeniu pracy przez użytkowników systemu/aplikacji, ww. elektroniczne nośniki informacji są przechowywane w meblach biurowych ze sprawnym zamknięciem lub w kasetkach.

7. Elektroniczne nośniki informacji, o których mowa powyżej, powinny być oznaczone w sposób umożliwiający ich identyfikację.
8. Elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą Osoby uprawnionej.
9. Dane osobowe na każdym nośniku informacji powinny być zabezpieczone przed odczytem (minimum hasłem).
10. Dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych.
11. Przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez ASI. Protokół należy przesłać do ABI.
12. Nośniki danych wykorzystywane do sporządzenia kopii nie mogą być stosowane do więcej niż:
    a. dyski CD-RW - 1000 cykli kopiowania
    b. pozostałe nośniki patrz zalecenia producenta.

VIII. Zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania.

1. Wszystkie kopie bezpieczeństwa oraz archiwa przechowywane są w sejfie.
2. Dostęp do sejfu mają tylko Osoby uprawnione.
3. Dostęp do danych archiwalnych mają tylko uprawnione osoby.
4. Zabezpieczenie Serwerowni opisane jest w Zasadach ochrony danych osobowych, stanowiących załącznik do niniejszej Instrukcji.
5. Zabezpieczenie systemu przetwarzania danych osobowych przed złośliwym oprogramowaniem opisuje Instrukcja zabezpieczenia antywirusowego systemu informatycznego, stanowiąca załącznik do niniejszego Dokumentu.

IX. Zasady i sposób odnotowywania informacji o udostępnionych i powierzonych danych osobowych.

1. Odnotowywane są informacje o odbiorcach danych z systemu.
2. Udostępnianie i powierzanie danych osobowych następują zgodnie z Zasadami ochrony danych stanowiącymi Załącznik nr Z-03 do Polityki.

3. Odnotowanie obejmuje informacje o:
   a) Nazwie jednostki organizacyjnej, imieniu, nazwisku osoby, której udostępniono dane
   b) Zakresie udostępnionych danych,
   c) Dacie udostępnienia.
4. Obowiązek odnotowania ww. informacji spoczywa na użytkowniku systemu, który dane udostępnia. Stosuje on w tym celu dostępne mu środki stosowane do organizacji pracy na jego stanowisku.
5. Odnotowanie powinno nastąpić niezwłocznie po udostępnieniu danych.

X. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system/aplikacja.
2. Przeglądy i konserwacja urządzeń:
   a. przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej dla danego systemu/aplikacji powinny być wykonywane w terminach określonych przez producenta sprzętu,
   b. jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decydują ASI,
   c. przegląd i konserwacja urządzeń, może być wykonana na żądanie Przełożonego,
   d. nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości ASI informuje IOD,
   e. za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada przełożony ASI.
3. Zasady zgłaszania awarii i udzielania pomocy opisuje Procedura postępowania w przypadku awarii systemu informatycznego służącego do przetwarzania danych osobowych, stanowiąca załącznik do niniejszej Instrukcji.
4. Sprzęt do naprawy jest przygotowywany i wywożony przez osobę upoważnioną przez ASI. Sprzęt taki musi uzyskać zgodę na naprawę od Osoby Uprawnionej.
5. Jeśli naprawa sprzętu lub oprogramowania musi zostać wykonana w miejscu przetwarzania danych osobowych albo na komputerze, gdzie są przetwarzane dane osobowe, to naprawy mogą być dokonywane w obecności Osoby uprawnionej.

6. Urządzenia przekazywane do naprawy do zewnętrznego serwisu należy pozbawić możliwości zapisu danych oraz możliwości ich odczytania przez nieupoważnione osoby, które dokonują naprawy.
7. W przypadku konieczności oddania sprzętu informatycznego do zewnętrznego serwisu ASI wymontowuje i zabezpiecza dysk twardy oraz inne nośniki danych zainstalowane w danym sprzęcie.
8. W przypadku konieczności oddania sprzętu informatycznego z nośnikami informacji ASI dokonuje zapisania danych na dysku sieciowym oraz nośniku CD lub DVD, a następnie kasuje dane Użytkownika w sposób uniemożliwiający ich odczytanie, ze względu na poufność danych zapisanych na dyskach użytkownika.
9. W przypadku awarii dysku twardego i konieczności podjęcia próby odtworzenia danych, zadanie to powierzane jest specjalistycznym firmom zewnętrznym, na podstawie zawartych umów.

Załączniki:

PROCEDURA NADAWANIA, ZMIANY, ODEBRANIA UPRAWNIEŃ UŻYTKOWNIKOWI	Z-01

SPIS TREŚCI

I. DEFINICJE

Polityka – Polityka Bezpieczeństwa.
Instrukcja – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych.
Wniosek – Wniosek o nadanie/zmianę/odebranie uprawnień do systemu informatycznego.
Karta użytkownika – Karta użytkownika stanowiąca załącznik do Instrukcji.
Oświadczenie – Oświadczenie użytkownika stanowiące załącznik do Polityki.
Administrator Danych Osobowych (Administrator) – Beskidzka Izba Lekarska reprezentowana przez Prezesa Okręgowej Rady Lekarskiej.
Inspektor ochrony danych (IOD) - osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie, zwany dalej IOD.
ASI – osoba uprawniona przez Administratora pełniąca obowiązki Administratora systemów informatycznych.
Użytkownik - osoba posiadająca upoważnienie wydane przez Administratora lub wyznaczoną przez niego osobę uprawnioną, dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.

II. OPIS PROCEDURY

Nadawanie uprawnień systemowych przeprowadza ASI. Powinno być zgodne z zasadą wiedzy koniecznej. Dostęp do serwera bazy danych powinien zostać ograniczony tylko do niezbędnego minimum. Wytyczne dotyczące zarządzania uprawnieniami Użytkownika:

W przypadku nowego Użytkownika

1. Przyjęcie i sprawdzenie 2 egzemplarzy wypełnionego Wniosku w części I, II i III
2. Uzupełnić datę wpływu wniosku i sygnaturę.
3. W przypadku wystąpienia wątpliwości z zakresu wnioskowanych uprawnień należy przesłać go do IOD.
4. W przypadku weryfikacji IOD, IOD uzupełnienia Wniosku w części IV.
    - jeżeli weryfikacja wniosku przez IOD jest odmowna zwracamy Wniosek osobie wnioskującej,
    - jeżeli IOD wyraża zgodę realizujemy procedurę od pkt.5.
5. Sprawdzić w Ewidencji użytkowników uprawnionych do przetwarzania danych osobowych podpisanie przez Administratora Upoważnienia dla użytkownika do przetwarzania danych osobowych oraz złożenie Oświadczenia użytkownika.
6. Nadać Identyfikator.
7. Założyć konto dostępu do sieci komputerowej w systemie FINN 7 SQL.
8. Wprowadzić uprawnienia do systemów zgodnie z Wnioskiem w części III z uwzględnieniem uwag IOD wykazanych w części IV.
9. Jeżeli uprawnienia są czasowe odnotować ten fakt we Wniosku.
10. Uzupełnić Wniosek w części V.
11. Sprawdzenie przez użytkownika poprawności dostępu do nadanych uprawnień.
12. Potwierdzenie przez użytkownika nadania uprawnień we Wniosku w części VI.
13. Wnioski ASI:

a. 1 egzemplarz przekazuje Kierownikowi Biura BIL w celu dołączenia do akt osobowych Pracownika lub jako załącznika do umów cywilnoprawnych,
b. 1 egzemplarz dołącza do prowadzonej ewidencji.

Czynności dla istniejącego użytkownika:

14. Wykonanie czynności w punktach od 1 do 4.
15. Wykonanie czynności w punktach od 8 do 13.

W przypadku zamknięcia (wygaśnięcia) uprawnień Użytkownika:

16. Wykonanie czynności w punktach od 1 do 2.
17. Zamknięcie lub zablokowanie kont do systemów.
18. Uzupełnić Wniosek w części V.
19. Wysłać kopię Wniosku do IOD.
20. Wnioski ASI:
    a. 1 egzemplarz przekazuje Kierownikowi Biura BIL w celu dołączenia do akt osobowych Pracownika lub jako załącznika do umów cywilnoprawnych,
    b. 1 egzemplarz dołącza do prowadzonej ewidencji.

WNIOSEK O NADANIE, ZMIANĘ, ODEBRANIE **) UPRAWNIEŃ DO SYSTEMU INFORMATYCZNEGO	**Z-02**

Sygnatura wniosku *)	……	**Data wpływu wniosku**	……

I. DANE PRZEŁOŻONEGO

Jednostka organizacyjna	……
Nazwisko i imię	……
Stanowisko / pełnione obowiązki **)	……
Podpis	……

II. DANE UŻYTKOWNIKA

Jednostka organizacyjna / nazwa firmy zewnętrznej **)	……
Nazwisko i imię	……
Stanowisko / pełnione obowiązki **)	……
Uprawnienia obowiązują od	……
Uprawnienia obowiązują do	……

III. ZAKRES UPRAWNIEŃ – wypełnia Przełożony

Lp	**System/program/aplikacja**	**Opis zakresu uprawnień**
1		
2		
3		
4		
5		
6		
7		

IV. WERYFIKACJA IOD – gdy jest to konieczne ze względu na zakres wnioskowanych uprawnień:

Data weryfikacji			…… ……
Nazwisko i imię			…… ……
	Decyzja		
	□ zgoda ***)	Uwagi do realizacji	…… ……
		……	
		……	
	□ odmowa ***)	Uzasadnienie odmowy	…… ……
		……	
		……	
	Podpis		…… ……
V. REALIZACJA WNIOSKU PRZEZ ASI			
Data			…… ……
Nazwisko i imię ASI			…… ……
Identyfikator nadany Użytkownikowi			
Uwagi związane z realizacją			…… ……
……			
……			
Podpis			…… ……
VI. POTWIERDZENIE UŻYTKOWNIKA NADANIA UPRAWNIEŃ			
Data			…… ……
Podpis			…… ……

**) wypełnia ASI*

***) niepotrzebne skreślić*

****) właściwą opcję zakreślić*

KARTA OPISOWA ZBIORU DANYCH ARCHIWALNYCH	Z-03
Nazwa zbioru	.....

I. DANE PODSTAWOWE

Data założenia	
Nazwisko i imię zakładającego	
Lokalizacja skryptu wykonującego	
Zawartość archiwum (pliki, baza danych, program)	
Miejsce składowania (serwer, katalog, nośnik danych)	
Nazwa zbioru archiwum (nazwa pliku)	
Stosowany program do kompresji	

II. KONTROLA KOPII BEZPIECZEŃSTWA

Data	Nazwisko i imię	Sprawdzenie wykonywania się kopii	Sprawdzenie odtworzenia kopii	Uwagi
1	2	3	4	5

INSTRUKCJA ZABEZPIECZENIA ANTYWIRUSOWEGO SYSTEMU INFORMATYCZNEGO	Z-04

I. DEFINICJE

Izba – Beskidzka Izba Lekarska.
Polityka – Polityka Bezpieczeństwa.
Oświadczenie – Oświadczenie użytkownika, stanowiące załącznik do Polityki.
Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
System informatyczny – sprzęt i programy komputerowe którego funkcją jest przetwarzanie danych osobowych.
Administrator danych osobowych (ADO, Administrator) – Beskidzka Izba Lekarska reprezentowana przez Prezesa Okręgowej Rady Lekarskiej.
Inspektor ochrony danych (IOD) - osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie, zwany dalej IOD.
ASI – osoba wyznaczona przez Administratora pełniąca obowiązki Administratora systemu informatycznego odpowiedzialna za wdrażanie technicznych zabezpieczeń systemów informatycznych, ich sprawność i konserwację oraz ochronę przetwarzanych w zbiorach danych osobowych.
Bezpieczeństwo systemu informatycznego – wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem Ustawy o ochronie danych osobowych, nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
Użytkownik - osoba posiadająca upoważnienie wydane przez Administratora lub wyznaczoną przez niego osobę uprawnioną dopuszczona do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu.
Przełożony - osoba pełniąca funkcję kierownika komórki organizacyjnej lub koordynatora będąca przełożonym użytkownika.
Opiekun - kierownik komórki organizacyjnej odpowiedzialny za dany zasób danych osobowych wynikający z zakresu pełnionych obowiązków.
Osoba uprawniona – osoba posiadająca upoważnienie wydane przez ADO lub osobę przez niego upoważnioną.

II. ZABEZPIECZENIE SPRZĘTOWE

1. Na styku sieci lokalnej z Internetem powinien być zainstalowane specjalizowane urządzenie do ochrony sieci zwane firewall-em.
2. Firewall powinien:

a) mieć możliwość zdefiniowania wielu różnych zestawów reguł określających jaki ruch powinien być przez firewall przepuszczany a jaki blokowany.

b) umożliwić filtrowania ruchu w godzinach pracy, innych w godzinach popołudniowych, a jeszcze innych w dni wolne od pracy

3. Wszystkie komputery znajdujące się w sieci powinny znajdować się za firewall-em.
4. W sieci Izby powinno być możliwe tworzenie tzw. kanałów VPN. Kanały te powinny umożliwić upoważnionym Użytkownikom bezpieczną pracę zdalną poza siedzibą *Izby.*
5. System informatyczny powinien być wyposażony w podstawowe usługi i serwisy sieciowe (DHCP, DNS, SNMP, NTP).
6. Sieć lokalna powinna wykorzystywać serwer proxy umożliwiający filtrowanie URL dla wszystkich lub wybranych grup użytkowników definiowanych przez *ASI*.
7. Administracja firewall-em i serwerem proxy powinna odbywać się z wykorzystaniem konsoli konfiguracyjnej.
8. ASI powinien mieć do dyspozycji monitor śledzący pracę systemu w czasie rzeczywistym oraz narzędzie raportujące, pozwalające na sporządzenie szczegółowych raportów.
9. Izba udostępnia dla wszystkich bezpłatny bez ograniczeń dostęp do sieci Internet w wydzielonej sieci bezprzewodowej dla wszystkich którzy korzystają z własnych urządzeń dostępowych.
10. Urządzenia służbowe (tablety) które wykorzystują sieci bezprzewodową muszą funkcjonować w chronionej, dedykowanej podsieci (VLAN-ie) i powinny być na nich wdrożone mechanizmy ochrony przed nieuprawnionym dostępem.
11. Serwery www świadczące usługi swobodnego dostępu z Internetu powinny być w wydzielonych strefach nie zabezpieczone firewall-em.

III. ZABEZPIECZENIE PROGRAMOWE

1. Każda stacja robocza lub serwer podłączony do sieci komputerowej w *Izbie* i posiadający dostęp do Internetu musi posiadać aktualne oprogramowanie antywirusowe oraz zaporę sieciową.
2. Oprogramowanie antywirusowe oraz zapora sieciowa muszą posiadać automatyczną aktualizację z sieci Internet lub z lokalnego repozytorium.
3. Oprogramowanie antywirusowe powinno wykrywać poza wirusami jak największą liczbę złośliwych programów innego rodzaju (np. konie trojańskie, backdoory, exploity, niebezpieczne aplety Javy i ActiveX, spam, itp.). Ponadto powinno charakteryzować się dobrymi narzędziami do analizy heurystycznej, skanowaniem na żądanie całości systemu bądź jego elementów, skanowaniem w czasie rzeczywistym i niskim obciążeniem systemu.
4. Oprogramowanie antywirusowe powinno posiadać funkcję automatycznego powiadamiania o wystąpieniu incydentu (np. pojawieniu się wirusa w poczcie, próby włamania do systemu, itp.), a także powinno monitorować system on-line i reagować na bieżąco na wszelkie incydenty wg stawionych przez *ASI* reguł.
5. Oprogramowanie antywirusowe powinno automatycznie sprawdzać wszelkie podłączane do systemu urządzenia.
6. Oprogramowanie antywirusowe oraz zapora sieciowa powinny być w języku polskim.
7. *Administrator* ma obowiązek przeznaczyć odpowiednie środki finansowe na *bezpieczeństwo systemu informatycznego*.

IV. OBOWIĄZKI ASI

1. *ASI* odpowiada za*:*

a) za aktualizację oprogramowania i jego baz na serwerach oraz lokalnych repozytoriach.

b) właściwą konfigurację oprogramowania antywirusowego oraz zapory sieciowej blokując wszystkie porty w zaporze sieciowej zezwalając tylko na komunikację aplikacji niezbędnych do pracy danemu *Użytkownikowi*

c) przeglądania i zabezpieczenia elektronicznie logów oprogramowania antywirusowego oraz zapory sieciowej.

d) przeszkolenie użytkowników mających w swoim zakresie obowiązków zabezpieczanie antywirusowe obsługi oprogramowania antywirusowego.

2. *ASI* ma obowiązek niezwłocznego reagowania na wszelkie powiadomienia o wystąpieniu incydentu, związanego z zainstalowanym oprogramowaniem antywirusowym i zaporą sieciową. zobowiązany jest podjąć właściwe działania dla danej sytuacji

3. *ABI* po otrzymaniu zgłoszenia o wystąpieniu incydentu od *ASI* i po zapoznaniu się ze sprawą, w wyniku której doszło do utraty (kradzieży)

4. *ASI* ma prawo wyłączyć użytkownikom mechanizm przeglądania i wysyłania treści wiadomości w formacie HTML w przeglądarce poczty.
W przeglądarkach internetowych ma prawo ograniczyć możliwości otwierania się różnego rodzaju skryptów.

5. *ASI* jest zobowiązany do sporządzania zestawu programów freeware akceptowalnych w sieci przez niego zarządzanej.

6. *ASI* ma obowiązek odnotowywania w elektronicznym dzienniku wszelkich incydentów, w wyniku których doszło do utraty/kradzieży danych lub innego przestępstwa, a także niezwłocznego zgłaszania tego faktu *ABI*. Ponadto administrator ma obowiązek zabezpieczyć logi dla celów dowodowych.

V. OBOWIĄZKI UŻYTKOWNIKA

1. Użytkownicy nie mogą instalować żadnego oprogramowania bez wiedzy i pisemnej zgody *ASI* lokalnej sieci komputerowej.

2. Użytkownicy nie mają prawa podłączać do sieci lokalnej uczelni żadnych urządzeń (np. routery, access pointy, switche, notebooki, palmtopy, kamery, aparaty fotograficzne, dyktafony cyfrowe, telefony komórkowe, pendrive, itp.), za wyjątkiem urządzeń służbowych, bez wiedzy i pisemnej zgody *ASI* ich sieci lokalnej.

3. Użytkownicy nie powinni otwierać poczty, załączników poczty oraz plików nieznanego pochodzenia. Dotyczy to również plików pobranych ze stron WWW (np. aplikacji flash, muzyki, krótkiego filmiku, itp.).

4. Każdy użytkownik powinien zostać przeszkolony w zakresie obsługi oprogramowania antywirusowego oraz zapory sieciowej, a także sposobów powiadamiania administratora sieci lokalnej o wystąpieniu incydentów (np. wirusów) wykrytych przez oprogramowanie antywirusowe. Użytkownicy nieprzeszkoleni mogą żądać przeprowadzenia stosownego szkolenia w ustalonym z administratorem terminie.

5. Po włożeniu zewnętrznego nośnika danych, jeśli nie zostanie on sprawdzony automatycznie przez oprogramowanie antywirusowe lub inne oprogramowanie chroniące, użytkownik ma obowiązek sprawdzenia go ręcznie przy pomocy w/w oprogramowania. System informatyczny powinien być tak zabezpieczony, aby uniemożliwić użytkownikowi korzystanie z zewnętrznych pamięci flash-wych jak również płyt CD/DVD.

6. W przypadku, gdy oprogramowanie powiadomi użytkownika o wystąpieniu incydentu (np. pojawieniu się wirusa, próbie włamania do systemu, itp.), użytkownik ma obowiązek postępować zgodnie z ustaleniami jakie uzyskał od administratora sieci lokalnej podczas szkolenia.

VI. ZASADY BEZPIECZEŃSTWA ANTYWIRUSOWEGO

Aby ograniczyć możliwość działania wirusów należy:

1. Diagnozować istnienie szkodliwego oprogramowania w trybie awaryjnym.
2. Sprawdzać listę uruchomionych programów i usług w menedżerze zadań (msconfig).
3. Ograniczać listę uruchamianych usług, z których korzysta się za pomocą sieci do minimum, tzn. do tych, z których rzeczywiście będzie się korzystać.
4. Stosować program antywirusowy i włączyć:

a) Zaporę,
b) Monitoring,
c) Automatyczne aktualizacje.

5. Szyfrować informacje.
6. Włącz automatyczne aktualizacje używanych programów, w szczególności systemu operacyjnego.
7. Nie udostępniać konta administratora użytkownikom.
8. Instalować oprogramowanie pochodzące z legalnego źródła oraz starać się, aby było ono jak najbardziej aktualne.
9. Instalować system operacyjny, gdy komputer jest odłączony od sieci i Internetu.
10. Podłączać komputer do Internetu dopiero wtedy, gdy sprawdzony ma skonfigurowane zabezpieczenia
11. Utworzone konta użytkowników zabezpieczać hasłem oraz ograniczyć ich uprawnienia.
12. Zmienić konto Administratora na inną nazwę lub wyłączyć konto Administrator, a jednemu z nowo utworzonych kont nadać uprawnienia administracyjne.
13. Ograniczyć do minimum współużytkowanie plików i drukarek w sieci.
14. Włączyć podstawowe zabezpieczenia systemu Windows - zaporę sieciową.
15. Ustawienie bezpiecznych stref bezpieczeństwa w przeglądarkach internetowych.
16. Stosowanie bezpiecznych haseł dostępu i innych rozwiązań uwierzytelniających wszędzie tam, gdzie jest to konieczne.
17. Bezpieczne usuwanie danych, których już się nie przetwarza (np. zastosowanie programu do bezpiecznego usuwania danych z nośników elektronicznych).
18. Regularnie archiwizować istotne dane (tworzenie kopii bezpieczeństwa).

PROCEDURA POSTĘPOWANIA W PRZYPADKU AWARII SYSTEMEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH	Z-05

I. DEFINICJE

Izba – Beskidzka Izba Lekarska
Użytkownik - osoba wykonująca zadania i obowiązki wynikające z umowy o pracę, umów cywilnoprawnych, umowy praktyki na rzecz Zakładu
Doraźny zbiór danych osobowych – zbiór danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych, a po ich wykorzystaniu niezwłocznie usuwany albo poddawany anonimizacji.
Inspektor ochrony danych (IOD) - osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie, zwany dalej IOD.
ASI – osoba uprawniona przez Administratora pełniąca obowiązki Administratora systemów informatycznych.

II. POSTĘPOWANIE W PRZYPADKU AWARII SYSTEMU INFORMATYCZNEGO

1. W przypadku wystąpienia awarii systemu informatycznego służącego do przetwarzania danych osobowych koniecznym jest niezwłoczne zgłoszenie jej ASI.
2. ASI po przyjęciu zgłoszenia awarii przystępuje do sprawdzenia systemu informatycznego.
3. W przypadku awarii, która może zostać naprawiona przez ASI przystępuje on do jej usunięcia.
4. W przypadku stwierdzeni awarii, której naprawa wymaga wezwania serwisu zewnętrznego, ASI bezzwłocznie informuje o tym serwis.
5. Na czas awarii systemu, z brakiem możliwości zalogowania do systemu, należy prowadzić zapisy w formie papierowej, tworząc doraźny zbiór danych osobowych.
6. Po usunięciu awarii Użytkownik w celu ponownego przystąpienia do pracy w systemie loguje się na swoje konto w komputerze i rozpoczyna pracę w systemie informatycznym.
7. Użytkownik wprowadza dane zgromadzone w zbiorze doraźnym stworzonym na czas awarii do systemu informatycznego.
8. Po wprowadzeniu danych zbiór doraźny ma zostać trwale zniszczony.

SEKRETARZ
OKRĘGOWEJ RADY LEKARSKIEJ

MACIEJ SKWARNA

WICEPREZES
OKRĘGOWEJ RADY LEKARSKIEJ

RADOSŁAW PIWOWARCZYK