Zatwierdzam

……

10.11.2021 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w

Eskulap Pabianice Prywatny Gabinet Lekarzy Specjalistów, Niepubliczny Zakład Opieki Zdrowotnej Eskulap Poradnia Zdrowia Rodzinnego Wioletta Sikora

Administrator Danych Osobowych

……..……

Pabianice. dnia 10 listopada 2021 r.

Rozdział I

Charakterystyka systemu

1. W Poradni istnieje wewnętrzna sieć informatyczna dla której działania wykorzystywany jest serwer firmy zewnętrznej, która świadczy Poradni usługę chmurową. W ramach sieci informatycznej podłączone są wszystkie komputery stacjonarne i przenośne Poradni wykorzystywane do przetwarzania danych osobowych.

2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i jest odpowiednio zabezpieczony.

3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie.

Rozdział II

Ogólne zasady pracy w systemie informatycznym.

1. Inspektor Ochrony Danych (IOD) wraz z Administratorami Systemu Informatycznego (ASI) Poradni odpowiadają za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian organizacyjno – funkcjonalnych w Poradni. W sytuacji zauważenia konieczności dokonania zmian w niniejszej instrukcji IOD lub ASI informują o tym Administratora (ADO).

2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez właściciela Poradni, jako Administratora, do eksploatacji licencjonowane oprogramowanie.

3. Wyznaczony ASI prowadzi ewidencję oprogramowania.

4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

a) mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika z pominięciem narzędzi do edycji tekstu,

b) mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizacje danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,

c) urządzenia niwelujące zakłócenia i podtrzymujące zasilanie.

5. Użytkownikom zabrania się:

a) udostępniania stanowisk roboczych osobom nieuprawnionym,

b) wykorzystania sieci komputerowej Poradni w celach innych niż czynności służbowe.

c) samowolnego instalowania i używania programów komputerowych,

d) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,

e) umożliwienia dostępu do zasobów wewnętrznej sieci informatycznej Poradni oraz sieci internetowej osobom nieuprawnionym,

f) używania komputera bez zainstalowanego oprogramowania antywirusowego.

Rozdział III

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

Nadawanie uprawnień

1. Administrator Danych Osobowych (ADO) w Poradni przyznaje uprawnienia w zakresie dostępu do danych osobowych na podstawie pisemnego upoważnienia.

2. Uprawnienia do przetwarzania danych osobowych są nadawane tylko i wyłącznie w zakresie wykonywanych przez pracownika zadań służbowych. Nadanie uprawnień polega na utworzeniu unikatowego identyfikatora użytkownika w systemie informatycznym Poradni.

3. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.

4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo poprzez zablokowanie konta użytkownika w przypadku np. podczas zawieszenia w pełnieniu obowiązków służbowych.

5. Uprawnienia do przetwarzania danych osobowych w Poradni odbierane są trwale w przypadku ustania stosunku pracy pracownika.

6. Jeżeli zachodzi konieczność modyfikacji nadanych uprawnień do przetwarzania danych osobowych w systemie informatycznym, zmiany dokonuje ADO, z własnej inicjatywy albo na wniosek IOD lub ASI, zgodnie z procedurą o której mowa w Polityce Bezpieczeństwa Przetwarzania i Ochrony Danych Osobowych obowiązującej w Poradni.

7. Osoby, które zostały upoważnione do przetwarzania danych osobowych są obowiązane zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia, tak w trakcie trwania zatrudnienia, jak i po ustaniu stosunku pracy.

8. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez wyznaczonego pracownika Poradni.

9. Wydane upoważnienia (oryginały) do przetwarzania danych osobowych w Poradni załączane są do akt osobowych pracowników.

10. Nadzór i kontrolę nad procesem rejestracji uprawnień do przetwarzania danych osobowych w systemie tradycyjnym tzw. dokumentacja papierowa przypisana jest IOD.

11. Nadzór i kontrolę nad procesem rejestracji uprawnień do przetwarzania danych osobowych w systemie informatycznym sprawuje ASI.

Rozdział IV

Osoby odpowiedzialne za nadawanie, modyfikacje, odbieranie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemach informatycznych

1. Kontrole przestrzegania niniejszej instrukcji przez pracowników Poradni wykonuje IOD.

Rozdział V

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

Przydział uprawnień i identyfikatorów

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych w Poradni posiada stosowne upoważnienie.

2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji z których musi korzystać w związku z realizacją obowiązków służbowych.

3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego Poradni polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora (loginu) oraz pierwszego hasła oraz określeniu zakresu dostępnych danych.

4. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika - ASI nadaje inny identyfikator, odstępując od ogólnej zasady.

5. Za gospodarkę loginami do programów informatycznych odpowiada ASI. Wymagania dotyczące hasła przedstawiają się następująco:

- autoryzacja w systemie operacyjnym odbywa się za pomocą hasła, które nie powinno zawierać mniej niż 9 znaków (używane małe i duże litery, cyfry oraz znaki specjalne),

- hasło nie może być takie samo jak identyfikator użytkownika systemu informatycznego,

- hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę,

- każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności,

- identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,

- hasła nie mogą być zapisywane w systemie w postaci jawnej,

- przy ustalaniu haseł nie mogą być używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,

- przy ustalaniu haseł nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

- hasło musi być zmieniane nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik systemu informatycznego.

- użytkownikowi nie wolno zapisywać hasła na papierze w postaci jawnej.

- użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,

- hasło przy wpisaniu nie może być wyświetlane na ekranie,

- zabronione jest stosowanie rozwiązań programowych pozwalających na zapamiętywanie identyfikatorów i haseł,

- hasło Administratora Systemu Informatycznego (ASI) Poradni przechowywane jest w opieczętowanej kopercie w miejscu wyznaczonym przez Administratora,

- hasło ASI musi być zmieniane nie rzadziej niż co 30 dni.

Rozdział VI

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

Procedura rozpoczęcia pracy

1. Przed rozpoczęciem pracy, w trakcie pracy oraz po jej zakończeniu należy zwrócić szczególną uwagę czy nie występują przesłanki mogące świadczyć o naruszeniu zasad ochrony danych osobowych.

2. Rozpoczęcie pracy użytkownika w systemie informatycznym Poradni obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła.

3. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami niemającymi uprawnień.

Procedura zawieszenia pracy

1. Opuszczając stanowisko pracy (stację roboczą komputera) użytkownik systemu informatycznego Poradni zobowiązany jest dokonać zamknięcia używanych programów służących do przetwarzania danych osobowych oraz zapisać wszystkie otwarte dokumenty.

2. W przypadku czasowego opuszczenia stanowiska pracy np. po 10 minutach powinien uruchomić się automatycznie wygaszacz ekranu zabezpieczający hasłem. Monitory komputerów usytuowane są w sposób uniemożliwiający odczytanie informacji z ekranu komputera osobom postronnym.

Procedura zakończenia pracy

1. Procedurę zakończenia pracy należy rozpocząć od zamknięcia wszystkich używanych programów służących do przetwarzania danych osobowych oraz zapisać wszystkie otwarte dokumenty.

2. Użytkownik systemu nie powinien opuszczać stanowiska pracy do chwili całkowitego wyłączenia komputera.

3. IOD oraz ASI monitorują logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

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

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.

2. Ochronie poprzez wykonywanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.

3. Kopie zapasowe baz danych stosowanych w Poradni, systemów informatycznych, programów, aplikacji sporządza się systematycznie.

4. ASI rejestruje sporządzanie kopii awaryjnych (zapasowych) w prowadzonym rejestrze w ujęciu chronologicznym, w przypadku, gdy kopie awaryjne (zapasowe) są i technicznie mogą być wykonywane na terenie Poradni. W pozostałym zakresie kopie awaryjne (zapasowe) wykonuje dostawca usług chmurowych, który jest właścicielem serwera.

5. Kopie awaryjne (zapasowe) mogą być wykonywane w Poradni tylko na nośnikach informatycznych zaakceptowanych przez ASI. Kopie wykonywane w Poradni przechowuje osoba wyznaczona przez ASI. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.

6. Kopie awaryjne (zapasowe) baz danych oraz ważnych plików wykonuje się w Poradni nie później niż do 15 następnego miesiąca. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu.

7. Kopie awaryjne (zapasowe) baz danych gromadzonych na serwerze przechowuje firma zewnętrzna jako dostawca usług chmurowych w zabezpieczonym miejscu.

8. Firma zewnętrzna jako właściciel serwera i dostawca usług chmurowych zobowiązana jest do okresowego wykonywania testów odtworzeniowych kopii zapasowych.

9. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.

10. Pracownicy użytkujący przenośne komputery w których przetwarzane są dane osobowe, zobowiązani są zachować szczególną ostrożność podczas transportu i przechowywania tego komputera. W celu zabezpieczenia ingerencji osób niepowołanych, dostęp do komputera należy zabezpieczyć hasłem i nie zezwalać na użytkowanie komputera osobom nieupoważnionym. Komputera przenośnego nie należy pozostawiać w samochodzie.

11. Zniszczenie kopii zapasowych na nośnikach magnetycznych i optycznych dokonuje ASI wyznaczony przez Administratora.

12. Z nośników wielokrotnego użytku dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.

13. Dane zawarte na nośnikach optycznych jednokrotnego użytku, np. płyty DVD lub CD, CDR należy usuwać poprzez całkowite zniszczenie nośnika.

Przetwarzanie danych osobowych

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.

2. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, zwłaszcza tzw. „dane wrażliwe" poza obszar przetwarzania danych osobowych, zabezpiecza się w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:

a) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi lub

b) stosowanie metod kryptograficznych lub

c) stosowanie odpowiednich zabezpieczeń fizycznych lub

d) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

3. Dane osobowe zapisywane na nośnikach zewnętrznych tworzące kopie zapasowe kolejnych okresów powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach w Poradni.

4. Kartoteki powinny być przechowywane w szafach znajdujących się w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.

5. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowane.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.

1. Nośniki danych, a także danych konfiguracyjnych systemu informatycznego, przechowuje się w odpowiednio w zabezpieczonym pomieszczeniu Poradni.

2. Za zgodą Administratora dane osobowe można przetwarzać na dyskach twardych komputerów stacjonarnych lub zarejestrowanych i służbowych nośnikach informacji dostarczonych przez ASI.

3. Przenośne nośniki danych powinny być obowiązkowo zabezpieczone ochroną kryptograficzną.

4. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do:

a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

b) przekazania podmiotowi nieuprawionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.

c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.

5. Nośniki kopii awaryjnych, które zostały wycofane z użycia podlegają zniszczeniu po usunięciu danych osobowych w odpowiednim urządzeniu niszczącym.

Rozdział VII

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

Komputery służące do przetwarzania danych osobowych w Poradni posiadają dostęp do sieci publicznej, wówczas system informatyczny narażony jest na oprogramowanie, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu. Stąd wprowadza się w systemie informatycznym Poradni wysoki poziom bezpieczeństwa przetwarzania danych osobowych.

Można wyróżnić następujące rodzaje występujących zagrożeń:

- nieuprawniony dostęp bezpośrednio do baz danych;

- uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu;

- przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesyłanie tych danych poza miejsce przetwarzania danych;

- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

W celu przeciwdziałania zagrożeniom system informatyczny Poradni powinien posiadać następujące zabezpieczenia:

- logowanie użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,

- użytkownicy systemu pracują wyłącznie na zbiorach danych osobowych do których posiadają upoważnienie wydane przez Administratora,

- dostęp do serwerów ma wyłącznie Administrator Systemów Informatycznych (ASI) i osoby upoważnione przez Administratora - zawsze w obecności ASI,

- zabronione jest pobieranie oraz instalowanie bez nadzoru ASI jakichkolwiek programów na wszystkich komputerach służących do przetwarzania danych osobowych;

- pracownicy nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i wolumenów z poziomu systemu operacyjnego;

- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych dla przetwarzania danych osobowych.

Potencjalnymi źródłami przedostania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,

- przeglądane strony internetowe,

- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

1. W celu zapewnienia ochrony antywirusowej wyznaczony przez Administratora ASI jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy.

2. Do ochrony antywirusowej należy stosować program antywirusowy zainstalowany na wszystkich komputerach.

3. Każdą przesyłkę otrzymaną za pomocą transmisji danych należy sprawdzić obowiązkowo programem antywirusowym. W celu zapewnienia maksymalnej ochrony program antywirusowy oraz jego baza są aktualizowane kilkukrotnie w ciągu dnia.

4. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchamianego pliku.

5. Użytkownicy są zobowiązani (lub system operacyjny wykonują tą czynność automatycznie) do dokonywania kontroli antywirusowej wszystkich nośników danych przychodzących z zewnątrz oraz okresowo własnych nośników danych.

6. Program antywirusowy zainstalowany na stacjach roboczych jest skonfigurowany w następujący sposób:

- zablokowana możliwość ingerencji użytkownika w ustalenia oprogramowania antywirusowego,
- możliwość centralnego uaktualniania wzorców wirusów.

7. Każdy pracownik przetwarzający dane osobowe przy użyciu komputera w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, powinien poinformować o tym fakcie ASI oraz IOD. W przypadku wykrycia wirusa choćby na jednym komputerze ASI jest zobowiązany sprawdzić wszystkie stacje robocze w Poradni.

Rozdział VIII

Informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

1. Informacje o udostępnieniu danych osobowych przetwarza się i przechowuje w oparciu o rzeczowy wykaz akt i instrukcje kancelaryjną.

2. Zgodę na udostępnienie danych osobowych może wydać wyłącznie Administrator.

3. Odpowiedzialność na udostępnienie danych osobowych zgodnie z przepisami prawa ponosi Administrator Danych Osobowych.

4. Nadzór nad właściwym udostępnianiem danych prowadzi Administrator.

Rozdział IX

Przesyłanie danych poza obszar przetwarzania

1. Urządzenia i nośniki zawierające dane osobowe obowiązkowo zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej (SZYFROWANIE DANYCH).

2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:

a) sprawdzeniu przez IOD zakresu danych osobowych przeznaczonych do wysłania,

b) zastosowanie mechanizmów szyfrowania danych osobowych (szyfrowanie załączanych plików zawierających dane osobowe),

c) zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych.

3. Umożliwienie wysyłania danych osobowych jest możliwe tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

Rozdział X

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

1. Przeglądy i konserwacje systemu Informatycznego oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora.

2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ASI.

3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ASI.

4. W przypadku konieczności przeprowadzenia prac serwisowych poza Poradnią dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.

5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.

6. Zabronione jest dokonanie napraw sprzętu komputerowego samodzielnie przez pracowników oraz użytkowników systemu informatycznego w Poradni. O wszelkich nieprawidłowościach lub awariach użytkownik systemu powinien niezwłocznie powiadomić Administratora Systemów Informatycznych (ASI) oraz Inspektora Ochrony Danych (IOD).

Rozdział XI

Procedura korzystania z internetu i poczty elektronicznej w Poradni

1. Celem procedury jest wskazanie zasad zapewnienia bezpieczeństwa dostępu i korzystania z internetu, w szczególności ze służbowej elektronicznej skrzynki pocztowej pracownika Poradni.

2. Użytkownicy systemu Informatycznego Poradni zobowiązani są do powiadamiania ASI oraz IOD o każdej nieprawidłowości użytkowania internetu, w szczególności poczty elektronicznej wykorzystywanej do celów służbowych przez pracownika Poradni.

3. ASI odpowiedzialny jest za tworzenie zasad optymalizujących i monitorujących generowany ruch wychodzący i wchodzący do wewnętrznej „LAN", zgłaszania prób łamania prawa, polityki bezpieczeństwa lub innych przyjętych w Poradni zasad dotyczących używania Internetu.

4. Administrator decyduję, w porozumieniu z ASI, czy pracownik powinien mieć ograniczony czy nieograniczony dostęp do Internetu lub też czy nie powinien mieć wcale dostępu do Internetu.

5. Z łączy internetowych należy korzystać w celu komunikowania się wyłącznie na temat działalności Poradni.

6. Administrator nie wyraża zgody na korzystanie przez pracowników Poradni w czasie wykonywania obowiązków służbowych w Poradni z internetu oraz z służbowej elektronicznej skrzynki mailowej w celach prywatnych.

7. Administrator za pośrednictwem ASI zastrzega sobie prawo do całkowitego monitorowania korzystania przez pracowników – użytkowników systemu informatycznego Poradni - z internetu, w szczególności korzystania ze służbowej elektronicznej skrzynki pocztowej.

8. Wszelkie informacje przechowywane na komputerach i w sieci są własnością Poradni i nie uważa się ich za własność prywatną.

9. Niewłaściwe korzystanie z łącza internetowego może doprowadzić do wszczęcia postępowania dyscyplinarnego, w celu wymierzenia kary porządkowej lub nawet zwolnienia z pracy. Ponadto, korzystanie z internetu dla celów niezgodnych z prawem może pociągnąć użytkowników do odpowiedzialności karnej.

10. Zabrania się przeglądania, zgrywania lub ujawniania informacji dostępnych przez internet, które Poradnia uznaje w jakikolwiek sposób za obraźliwe lub niebezpieczne dla wewnętrznych systemów informatycznych.

11. Zabrania się czerpania korzyści osobistych lub prowadzenia działalności gospodarczej wykorzystując dostęp do Internetu w Poradni.

12. Zabrania się przekazywania na zewnątrz poufnych informacji oraz łamania prawa.

13. Zabrania się zgrywania aplikacji i danych z internetu bez poprzedniego uzyskania zgody ASI.

14. Zabrania się korzystania z osobistych kont pocztowych.

15. Zabrania się nieuzasadnionego – nie związanego z wykonywanymi służbowymi obowiązkami - nadmiernego korzystania z internetu powodując tym samym niepotrzebne obciążenie łącza.

16. Administrator zastrzega sobie prawo do wglądu w służbową pocztę elektroniczną pracowników Poradni, jeżeli są ku temu podstawy tzn. dla celów bezpieczeństwa, kiedy jest to wymagane przez prawo lub jako element śledztwa. Każdorazowy wgląd w pocztę elektroniczną pracownika musi zostać wcześniej zapowiedziany w sposób jasny i zrozumiały dla użytkownika systemu Informatycznego w Poradni.

17. Jeżeli poufne lub zastrzeżone informacje mają być wysłane pocztą elektroniczną powinny one być zakodowane – np.: spakowane z hasłem.

18. Przychodzące wiadomości kontrolowane są automatycznie z wykorzystaniem specjalistycznego oprogramowania pod względem obecności wirusów i innej niepożądanej zawartości, która mogłaby uszkodzić systemy firmy lub w inny sposób negatywnie na nie wpłynąć lub zmniejszyć wydajność.

19. Niewłaściwe użycie poczty elektronicznej w Poradni może doprowadzić do wszczęcia postępowania dyscyplinarnego, a czynności zakazane prawem są przestępstwem i mogą doprowadzić do postępowania karnego.

20. Przesyłanie informacji za pośrednictwem poczty elektronicznej powinno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z

dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z IOD lub z ASI.

21. Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy treści maila załączonego dokumentu zawierającego dane osobowe.

22. Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik powinien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją. Adresat zobowiązany jest w takiej sytuacji przesłać nadawcy potwierdzenie.

23. Informacje przesyłane za pośrednictwem poczty elektronicznej muszą być zgodne z prawem i z zasadami obowiązującymi w Poradni.

24. Użytkownicy posiadają zakaz na odbieranie przesyłek elektronicznych (korespondencji mailowej, w szczególności załączników) od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki, użytkownik powinien ją zniszczyć lub skontaktować się z ASI.

25. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu ASI, który winien sprawdzić czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji.

26. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp.

27. Użytkownicy nie powinni rozsyłać wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów - określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej

28. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

29.Korzystanie z poczty według uznania Poradni jest przywilejem, który może zostać w każdej chwili wycofany.

30. Imię i nazwisko użytkownika, adres i inne podobne informacje przesyłane wraz z wiadomościami rzutują na wizerunek Poradni. Użytkownicy nie mogą zmieniać, przeinaczać, ukrywać lub zamieniać się swoimi danymi identyfikacyjnymi w czasie wysyłania wiadomości.

Rozdział XII

Postanowienia końcowe

1. Wobec osoby działającej w imieniu Poradni, pracownika Poradni, który w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjął działania określonego w niniejszym dokumencie, a w szczególności nie powiadomił odpowiedniej osoby zgodnie z określonymi zadaniami, a także gdy nie zrealizował stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie interdyscyplinarne.

2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być traktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Inspektora Ochrony Danych (IOD).