Księga procedur bezpieczeństwa

Sporządził:		Zatwierdził:	
Pełnomocnik ds. ZSZ	mgr inż. Mirosław Dereń	Dyrektor	płk dr hab. n. med. Ewelina Zawadzka-Bartczak
Podpis:		Podpis:	
Data :	24.07.2018	Data :	26 LIP. 2018
Wydanie:	4.1	Wydanie 1.0 wprowadzone zostało Zarządzeniem Dyrektora WIML Nr 9/2011	

Spis treści

Struktura zarządzania bezpieczeństwem i podział odpowiedzialności

Dyrektor

- całość bezpieczeństwa informacji;
- nadawanie i odbieranie uprawnień do przetwarzania danych osobowych,
- odpowiada za wyrażanie zgody na udostępnienie stronom trzecim informacji stanowiących tajemnicę WIML.
- decydowanie o współpracy w zakresie bezpieczeństwa z innymi podmiotami;

Pełnomocnik ds. Zintegrowanego Systemu Zarządzania (ZSZ)

- odpowiada za nadzór nad realizacją Polityki Bezpieczeństwa Informacji oraz innych dokumentów wewnętrznych związanych z ochroną informacji;
- identyfikuje i dokumentuje zagrożenia zachowania bezpieczeństwa informacji,
- definiuje oraz śledzi realizację działań zapobiegających zagrożeniom,
- uczestniczy w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa;
- koordynuje działania ukierunkowane na zapewnienie bezpieczeństwa informacji oraz aktualizację związanych z nim polityk i procedur;
- przeprowadzi szkolenia w zakresie bezpieczeństwa informacji dla osób upoważnionych do korzystania z informacji objętych ochroną;
- wskazuje właścicieli aktywów;
- kontroluje znajomość procedur bezpieczeństwa przez wszystkich użytkowników systemu w zakresie bezpieczeństwa teleinformatycznego, w odniesieniu do ochrony informacji na stanowiskach pracy;
- podejmuje odpowiednie działania w przypadku wykrycia naruszeń bezpieczeństwa informacji lub prób takich naruszeń;
- rozstrzyga problemy dotyczące wątpliwości w stosowaniu dokumentacji systemu;
- uczestniczy w planowaniu szkolenia z zakresu bezpieczeństwa informacji i teleinformatycznego;

Administrator Systemu Informatycznego odpowiada za:

- całość bezpieczeństwa informacji w ogólnych systemach i sieciach informatycznych;
- nadzór i kontrolę uprawnień do korzystania z danych w systemach informacyjnych
- zapewnienie przetwarzania danych osobowych zgodnie z Ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. oraz innymi przepisami powszechnie obowiązującego prawa;

- monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych oraz dostosowanie systemu do wymagań prawnych;
- uczestnictwo w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa;
- nadzór i kontrolę konfiguracji systemu w zakresie dostępu do sieci teleinformatycznej;
- prowadzenie bieżącej kontroli zabezpieczeń oraz zgodność funkcjonowania systemu ze szczególnymi wymaganiami bezpieczeństwa;
- wdrażanie procedur ochrony antywirusowej, przed złośliwym oprogramowaniem oraz nieuprawnionym dostępem do zasobów systemów za pośrednictwem sieci teleinformatycznych;
- sprawdzanie poprawności działania systemu oraz jego zabezpieczeń w zakresie ochrony antywirusowej, przed złośliwym oprogramowaniem oraz innymi zagrożeniami mogącymi pochodzić z sieci teleinformatycznych;
- proponowanie zmian mających na celu zwiększenia bezpieczeństwa systemu lub sieci teleinformatycznej;
- nadzór procesu sporządzania kopii zapasowych danych znajdujących się w systemach teleinformatycznych.

Administrator Systemu Informatycznego, Pełnomocnik ds. ZSZ, Pełnomocnik ds. OIN, Inspektor Ochrony Danych oraz właściciele aktywów koordynują działania w zakresie bezpieczeństwa poprzez:

- wskazywanie kierunków działań w zakresie bezpieczeństwa;
- wykonywanie przeglądów Polityki Bezpieczeństwa Informacji;
- monitorowanie istotnych zmian narażenia aktywów informacyjnych na podstawowe zagrożenia;
- wykonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informacji;
- spotkania na przeglądach zarządzania oraz doraźne w sytuacjach mogących mieć istotny wpływ na bezpieczeństwo informacji;
- analizowanie istotnych zmian narażenia aktywów informacyjnych na zagrożenia;
- dokonywanie analizy naruszeń bezpieczeństwa informacji.

Właściciele aktywów – odpowiadają za:

- bezpieczeństwo informacji w zakresie nad którym sprawują nadzór;
- przeciwdziałanie dostępowi do informacji chronionych osób niepowołanych;
- wnioskowanie o wskazaniach do współpracy w zakresie bezpieczeństwa z innymi podmiotami, w zakresie nad którym sprawują nadzór;

- wyrażanie zgody, po uzyskaniu zezwolenia Dyrektora, na udostępnienie stronom trzecim informacji chronionych należących do aktywa, którego są właścicielami;
- zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy;
- podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie;
- zapewnienie przetwarzania danych osobowych zgodnie z Ustawą o ochronie danych osobowych;
- bieżące nadzorowanie oraz zarządzanie aktywami jako właściciele aktywów;
- nadzór nad poprawnością pracy użytkowanych systemów informatycznych oraz mechanizmów zabezpieczających dane w tych systemach;
- nadzór nad zabezpieczeniem danych poprzez tworzenie i właściwe zabezpieczanie kopii zapasowych;
- analizę pracy użytkowanych systemów informatycznych w celu wykrycia potencjalnych zagrożeń;
- nadzór nad przeprowadzaniem, w bezpieczny sposób, napraw oraz konserwacji sprzętu i oprogramowania służącego do przetwarzania lub będącego nośnikiem danych;
- utrzymywanie ochrony aktywów i zasobów, którymi dysponują;
- wprowadzanie zabezpieczeń;
- utrzymanie aktualnych wersji oprogramowania oraz dokumentacji eksploatacyjnej;
- wnioskowanie o nadanie lub odebranie uprawnień oraz prowadzenie ewidencji nadanych uprawnień do dostępu do informacji chronionych;
- prowadzenie dokumentacji systemu;
- organizowanie szkoleń z zakresu bezpieczeństwa informacji dla osób upoważnionych do korzystania z informacji objętych ochroną;
- przegląd i weryfikację efektywności ustanowionego systemu i informowanie podczas przeglądu o jej wynikach;
- autoryzację zakupów sprzętu i oprogramowania pod kątem zgodności z zasadami systemu bezpieczeństwa informacji;
- współpracę z **Pełnomocnikiem ds. ZSZ** oraz innymi **Właścicielami Aktywów** w zakresie realizacji zadań dotyczących bezpieczeństwa informacji;
- propagowanie zasad Systemu Zarządzania Bezpieczeństwem Informacji wśród pracowników w podległych im obszarach;
- nadzorowanie realizacji założeń Polityki Bezpieczeństwa Informacji i innych dokumentów systemu bezpieczeństwa informacji w podległych obszarach.

Pracownicy

- Odpowiedzialność za bezpieczeństwo informacji w WIML, ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. **Każdy pracownik zobowiązany jest dbać o bezpieczeństwo** powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi w WIML przepisami wewnętrznymi w tym między innymi:
- stosować zasady opisane w politykach oraz innych dokumentach wewnętrznych WIML;
- chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;
- chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
- chronić sprzęt, nośniki informacji (różnego rodzaju pamięci i wydruki, formularze, zdjęcia) zawierające chronione dane;
- utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów, także po ustaniu zatrudnienia w WIML;
- stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z Zintegrowanego Systemu Zarządzania;
- powiadomić Pełnomocnika ds. ZSZ, właściciela aktywa, Inspektora Ochrony Danych (w przypadku danych osobowych) lub bezpośredniego przełożonego o:
    - ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym;
    - nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian;
    - zniszczeniu lub możliwości zniszczenia informacji chronionych;
    - zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych;

Zabrania się pod rygorem odpowiedzialności służbowej i karnej:

- ujawniać informacje chronione (w tym dane osobowe),
- kopiować chronioną dokumentację, bazy danych lub ich części poza kopiami przewidzianymi dokumentacją Zintegrowanego Systemu Zarządzania jak np. kopie bezpieczeństwa,
- uszkadzać lub niszczyć sprzęt lub informacje bez zachowanych odpowiednich procedur bezpieczeństwa,
- zabrania się przetwarzania informacji chronionych w sposób mogący narażać na utratę bezpieczeństwa tych danych przez naruszenie poufności, integralności lub dostępności,
- instalowania oprogramowania niezwiązanego z wykonywaniem obowiązków służbowych.

Współpraca

Zasady współpracy z osobami trzecimi

Osoby przebywające na terenie WIML, nie będące pracownikami są zobowiązane do przestrzegania następujących zasad:

- reguł bhp;
- reguł bezpieczeństwa przeciwpożarowego;
- wpisania się w księdze gości, tam gdzie jest to wymagane.

Każda osoba nie będąca pracownikiem WIML, która wykonuje prace zlecone, z którymi wiąże się dostęp do informacji chronionych przez WIML zobligowana jest do podpisania oświadczenia o zachowaniu poufności, bądź stosownej umowy.

Osoby niezatrudnione w WIML mogą otrzymać od Dyrektora, Pełnomocnika ds. OIN lub właściciela aktywa prawo dostępu fizycznego lub/i logicznego do informacji, jeżeli

- jest to niezbędne do realizacji obowiązków WIML, wobec klientów lub do bieżącego funkcjonowania WIML;
- dają one gwarancję zachowania poufności;
- podpisały z WIML oświadczenie o zachowaniu tajemnicy przedsiębiorstwa lub umowę określającą odpowiedzialność za naruszenie poufności.

Osobom tym powinno zostać odebrane prawo dostępu po wygaśnięciu przyczyny udzielenia ww. dostępu np. po wykonaniu zleconej pracy.

Zasady współpracy z innymi podmiotami

Współpraca WIML, z innymi osobami fizycznymi i prawnymi oparta jest na umowach cywilno-prawnych. Zawierając te umowy WIML uwzględnia wymaganą deklarację o zachowaniu bezpieczeństwa informacji i przestrzeganiu zasad bezpieczeństwa informacji przyjętych w WIML.

Polityka kontroli dostępu

Kontrola dostępu do pomieszczeń biurowych.

Pomieszczenia biurowe w WIML, zamykane są na klucz. Każdy pracownik odpowiada za zamykanie pomieszczeń i za swój klucz. W przypadku zagubienia klucza należy niezwłocznie poinformować o tym fakcie przełożonego.

Kontrola dostępu do serwerowni.

Na terenie WIML znajduje się obszar wydzielony z uwagi na pomieszczenia chronione w szczególny sposób. Dostęp ten jest kontrolowany przez Administratora Danych. Sprzątanie w tym obszarze odbywa się tylko w obecności upoważnionych pracowników.

Zasady nadawania uprawnień użytkowników

Udzielanie, zmiana i odbiór uprawnień użytkowników jest wykonywane przez, lub na wniosek właściciela aktywa lub na wniosek jego przełożonego. Wniosek (formularz WIML-ZSZ-24) musi zawierać: imię i nazwisko, stanowisko, zakres uprawnień do poszczególnych systemów i zasobów, jaki ma posiadać dany użytkownik. Wnioski mają formę papierową. Upoważnieni pracownicy gromadzą dokumentację związaną z nadawaniem i odbiorem uprawnień.

Nadanie uprawnień administratora do danego systemu informatycznego aktywa wymaga akceptacji właściciela aktywa.

W przypadku rejestrowania konta nowego użytkownika w systemie, identyfikator i hasło początkowe musi mu być przekazane w sposób uniemożliwiający użycie tych informacji przez osoby nieuprawnione. Nowy użytkownik jest zobowiązany do zmiany hasła już przy pierwszym zalogowaniu do systemu.

Zasady i korzystanie z haseł w systemach informatycznych

Dostęp do systemu informatycznego przetwarzającego chronione dane możliwy jest wyłącznie dla zarejestrowanych użytkowników po podaniu identyfikatora oraz hasła. Identyfikator jest unikalny dla każdego użytkownika systemu.

Hasło jest znane tylko przez użytkownika, z wyjątkiem hasła tymczasowego nadawanego przez Administratora danego systemu.

Hasło powinno zawierać, co najmniej **8 znaków** w przypadku systemów przetwarzających dane wrażliwe (w tym osobowe) i być zmieniane co **30 dni roboczych**, oraz co najmniej **6 znaków**, zmiana co 6 miesięcy - jeżeli użytkowane systemy posiadają taką możliwość i nie przetwarzają danych wrażliwych.

Hasło nie powinno być słowem łatwym do zidentyfikowania jak np. imieniem, nazwiskiem, datą urodzenia, numerem telefonu itp. Użytkownik hasła zobowiązany jest do:

- nieujawniania hasła innym osobom,
- zachowania hasła w tajemnicy również po wygaśnięciu jego ważności,
- niezapisywania hasła w miejscach dostępnych dla osób nieuprawnionych,
- przestrzegania zasad dotyczących złożoności haseł,
- wprowadzania hasła w sposób minimalizujący ryzyko podejrzenia go.

Zasady korzystania z systemów informatycznych

Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie bezpieczeństwa informacji. W przypadku naruszenia bezpieczeństwa informacji użytkownik postępuje zgodnie z polityką zarządzania incydentami.

Użytkownik rozpoczyna pracę w systemie informatycznym od uwierzytelnienia się („zalogowania" w systemie) za pomocą swojego identyfikatora i hasła.

Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.

Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności nośniki wymienne, dokumenty i wydruki zawierające ważne dane, przed dostępem osób nieupoważnionych zgodnie z polityką czystego biurka i ekranu.

Oprogramowanie

Oprogramowanie może być instalowane przez Użytkowników na komputerach **tylko i wyłącznie** po uzyskaniu zgody osoby odpowiedzialnej za legalność oprogramowania. Oprogramowanie może być wykorzystywane **tylko i wyłącznie do użytku służbowego**.

Poczta elektroniczna

Jeżeli Użytkownik korzysta z konta pocztowego (e-mail), to może je wykorzystywać **tylko i wyłącznie do użytku służbowego**. Wszelka wpływająca korespondencja prywatna musi zostać bezzwłocznie usunięta.

Zasady pracy na odległość

Praca na odległość możliwa jest tylko za zgodą przełożonego oraz właściciela aktywów, które będą w tej pracy wykorzystywane.

Praca na odległość może być wykonywana tylko wtedy, gdy są wdrożone stosowne ustalenia i zabezpieczenia oraz zapewniono ich zgodność z polityką bezpieczeństwa WIML.

Praca na odległość stron zewnętrznych wymagająca zdalnego dostępu do aktywów WIML, regulowana jest odpowiednimi umowami i instrukcjami eksploatacyjnymi systemów pracujących w trybie zdalnego dostępu z zastosowaniem stosownych zabezpieczeń.

Okresowa kontrola praw dostępu

Właściciel aktywa **nie rzadziej niż raz w roku** przeprowadza **kontrolę aktualności** i poprawności listy zarejestrowanych w systemie użytkowników i przypisanych im praw dostępu. Przegląd odbywa się poprzez porównanie faktycznie istniejących kont z zatwierdzonym, przez właścicieli aktywów, wykazem użytkowników.

Eksploatacja systemów i sieci

Użytkownik podczas pracy w systemie informatycznym sprawdza na bieżąco poprawność działania systemu i informuje o wszelkich nieprawidłowościach informuje W przypadku naruszenia bezpieczeństwa informacji użytkownik postępuje zgodnie z polityką zarządzania incydentami.

Administratorzy użytkowanych systemów informatycznych wykonują okresowe przeglądy zasobów wykorzystywanych przez nadzorowane aplikacje oraz dokonują aktualizacji oprogramowania lub wysyłają komunikaty o obowiązku przeprowadzenia aktualizacji np. programów antywirusowych.

W ramach przeglądu sprawdzane są logi systemowe, logi baz danych, wykorzystanie pojemności dysków i innych zasobów pamięci oraz zapełnienie przestrzeni przeznaczonej na poszczególne zbiory (tabele) baz danych.

W przypadkach przekroczenia optymalnych parametrów podejmują działania zwiększające przydział zasobów do aplikacji.

Wszystkie urządzenia, których praca wpływa na ciągłość pracy on-line są zabezpieczone przed awarią zasilania za pomocą urządzeń UPS, pozwalających na zamknięcie aplikacji, systemów narzędziowych i operacyjnych, oraz ich podniesienie po powrocie zasilania.

Konta pocztowe

Konta pocztowe przyznawane są zgodnie z polityką kontroli dostępu do systemów i sieci.

W przestrzeni adresowej WIML występują również grupy użytkowników posiadające adresy grupowe. Przynależność użytkownika do grupy wynika z wykonywania powierzonych obowiązków i struktury organizacyjnej.

Zasady bezpieczeństwa informacji przy korzystaniu z poczty elektronicznej

Bezpieczeństwo informacji przy korzystaniu z poczty elektronicznej zależy w znacznej mierze od ustawień programu obsługującego pocztę oraz od działania samego użytkownika.

Każdy użytkownik, który uzyskał uprawnienia do korzystania z poczty elektronicznej jest zobowiązany przynajmniej jeden raz w ciągu dnia odczytać dostarczoną pocztę. Dotyczy to dni jego obecności w pracy. W przypadku nieobecności w pracy powinien podjąć działania,

żeby zminimalizować negatywny wpływ nieobecności na wymianę informacji (poinformowanie ważnych nadawców, odpowiednie ustawienia automatyki programu pocztowego).

Należy pamiętać o tym, że informacja przesyłana pocztą elektroniczną jest łatwa do odczytania przez osoby, dla których nie została przeznaczona. W przypadku istnienia potrzeby ochrony przesyłanej informacji przed nieuprawnionym dostępem, należy stosować odpowiednie do sytuacji środki bezpieczeństwa (hasła, szyfrowanie, podpis elektroniczny).

Przy przesyłaniu załączników należy uwzględnić fakt, że skrzynki pocztowe mają ograniczoną pojemność i dostosować do niej rozmiary przesyłek (kompresja, podział przesyłki na części) oraz czas przechowywania informacji (czyszczenie skrzynek).

Wysłanie wiadomości pocztą elektroniczną nie gwarantuje, że dotrze ona do adresata i zostanie przez niego przeczytana. W przypadku, gdy dostarczenie jej jest istotne z biznesowego punktu widzenia, należy zastosować wbudowane w system pocztowy mechanizmy potwierdzenia odbioru i przeczytania przesyłki lub zażądać potwierdzenia tego faktu przez adresata.

Ze względu na to, że nadawca poczty może stosunkowo łatwo podszyć się pod kogoś innego (jeżeli poczta nie jest podpisana odpowiednim podpisem elektronicznym), należy przy przesyłkach budzących wątpliwości a istotnych biznesowo potwierdzić inną drogą tożsamość nadawcy.

Przy kierowaniu wiadomości do kilku odbiorców należy się upewnić, czy życzą oni sobie by ich adresy e-mail były wzajemnie udostępniane, i na tej podstawie wybrać odpowiedni sposób adresowania: do (to), do wiadomości - (cc), ukryta kopia do (bcc). Stosując ostatni wariant unikamy ujawniania adresów e-mail poszczególnym adresatom jednej wiadomości.

Zalecany sposób korzystania z poczty elektronicznej:

- stosowanie hasła dostępu do klienta poczty chroniącego przed nieupoważnionym dostępem do wiadomości użytkownika,
- wyłączenie automatycznego podglądu wiadomości,
- wyłączenie automatycznego otwierania kolejnej wiadomości,
- wyłączenie uruchamiania aktywnych elementów,
- wyłączenie automatycznego pobierania plików graficznych w wiadomościach HTML,
- wyłączenie funkcji zapamiętywania haseł ,
- aktywowanie filtrów;
- nie należy odpowiadać na przesyłki ani otwierać załączników w przesyłkach o podejrzanych adresach nadawcy;
- nie należy przekazywać w odpowiedzi na przesyłkę żadnych danych osobistych, finansowych lub biznesowych bez sprawdzenia tożsamości nadawcy i rzeczywistego celu przekazania takich informacji;
- nie należy używać linków internetowych w przesyłkach od niepewnych nadawców.

Ochrona systemowa poczty przychodzącej

Poczta przychodząca i wychodząca jest kontrolowana na komputerach klienckich i na serwerze komercyjnymi środkami antywirusowymi i antyspamowymi.

Zabronione jest wyłączanie ochrony bez zgody osoby upoważnionej!

Archiwizowanie poczty

Skrzynki pocztowe użytkowników przechowywane powinny być na serwerze. Takie skrzynki objęte są ogólną polityką backupów. Za zabezpieczenie skrzynek przechowywanych lokalnie odpowiadają użytkownicy.

Zarządzanie wymiennymi nośnikami

Wymienne nośniki informacji muszą być opisane w sposób umożliwiający identyfikację zawartości nośnika, jeśli posiadają informacje chronione, nie mogą one być wynoszone poza siedzibę WIML bez zgody przełożonego.

Zaleca się wymazanie poprzedniej zawartości wszelkich nośników wielokrotnego użytku, które mają być wyniesione z WIML, o ile zawartość ta nie będzie już potrzebna.

Wymienne nośniki informacji muszą być transportowane i przechowywane w sposób zabezpieczający przed dostępem osób nieuprawnionych oraz utratą nośnika bądź informacji na nim zapisanej.

Korzystanie z wymiennych nośników informacji powinno się odbywać z uwzględnieniem ochrony ich zawartości przed złośliwym lub szkodliwym oprogramowaniem.

Jako zasadę przyjmuje się trwałe niszczenie nośników zawierających informacje chronione tak, aby nie był możliwy odczyt z nich jakichkolwiek danych, jeżeli używanie ich nie jest już uzasadnione lub zostały one uszkodzone np.: przez fizyczne zniszczenie nośnika.

Przed przekazaniem innemu, nieuprawnionemu pracownikowi komputerów lub dysków zawierających dane chronione, zawarte na przekazywanych nośnikach dane są nieodwracalnie usuwane w sposób uniemożliwiający ich ponowne odtworzenie lub odczytanie np.: przez formatowanie lub nadpisanie innymi danymi.

Kopie zapasowe

Zasadniczym celem wykonywania kopii zapasowych jest zabezpieczenie danych przed utratą wynikłą z awarii sprzętu lub niewłaściwego użycia (skasowanie, niewłaściwa zmiana zawartości). Wykonywane są kopie zapasowe jedynie danych o istotnym znaczeniu.

Rodzaje danych, dla których wykonywane są kopie bezpieczeństwa:

- Dane własne WIML, pochodzące z systemów informatycznych – za wykonywanie kopii odpowiedzialny właściciel aktywa. Zalecane jest tworzenie kopii nie rzadziej niż raz w tygodniu,
- Dane ze stacji roboczych pracowników składowane na udostępnianych serwerach w przypadku zgłoszenia przez pracownika takiej potrzeby:
  - Konto na serwerze udostępniane jest zgodnie z polityką dostępu do systemów i sieci,
  - Za składowanie danych na serwerze odpowiedzialny jest administrator. Udostępniony serwer jest dodatkowym, bezpiecznym miejscem przechowywania ważnych danych,
  - Konta na serwerze są chronione identyfikatorem i hasłem użytkownika,

Nośniki na których wykonywane są kopie zapasowe usytuowane są w pomieszczeniach Serwerowni – dostęp do nich mają jedynie uprawnieni pracownicy.

Dodatkowo, okresowo, wykonywana jest kopia danych z serwerów działu IT na nośniku przechowywanym w kancelarii Punktu Ewidencyjnego WIML:

- Dane na stacjach roboczych pracowników
  - Kopie zapasowe danych na stacjach roboczych są wykonywane, przechowywane i sprawdzane przez ich użytkowników zgodnie z indywidualnymi potrzebami,
  - Nośniki zawierające kopie informacji chronionych, w tym dane osobowe, należy chronić w sposób szczególny, aby uniemożliwić dostęp do nich osobom nieupoważnionym, kradzież lub zagubienie. Za ochronę tych nośników odpowiadają sporządzający kopie na tych nośnikach,
  - Wycofane z użycia wymienne nośniki z kopiami zapasowymi uszkadza się w sposób uniemożliwiający odczytanie danych przez fizyczne zniszczenie zgodnie z zarządzaniem nośnikami wymiennymi.

Polityka postępowania z informacją

Informacja (w postaci aktywów informacyjnych) jest sklasyfikowana zgodnie ze stawianymi jej wymaganiami w zakresie ochrony. Określone zostały zasady postępowania z danymi grupami informacji oraz grupy pracowników posiadające do nich dostęp.

Zasady postępowania dotyczące bezpieczeństwa informacji odnoszą się do informacji chronionych. Informacje chronione to wszystkie aktywa informacyjne wskazane w analizie ryzyka. Osobami mającymi dostęp do informacji chronionych są upoważnieni pracownicy WIML, dla których dane informacje są niezbędne do wykonywania obowiązków służbowych oraz osoby spoza WIML, którym interes WIML wymaga udostępnienia danych informacji. Upoważnieni pracownicy posiadają indywidualne konta w systemach informatycznych, ustalony dostęp do poszczególnych pomieszczeń i tym samym dostęp do informacji.

Każdy użytkownik informacji chronionej ma obowiązek postępowania z nią zgodnie z poniższymi zasadami:

Zasada poufności informacji

- nie udostępnianie informacji osobom nieupoważnionym (zarówno pracownikom WIML, jak i osobom trzecim),
- korzystanie z informacji w taki sposób, aby udaremnić dostęp do niej osób nieupoważnionych,
- odpowiednia ochrona informacji podczas jej przechowywania i przesyłania.

Zasada integralności informacji

- zabezpieczenie informacji przed niepożądaną, a także nieautoryzowaną zmianą, zniekształceniem lub usunięciem części lub całości informacji,

Zasada dostępności informacji

- przechowywanie i dystrybucja informacji w taki sposób, aby była dostępna dla osób upoważnionych zawsze, gdy jest potrzebna (ustalone miejsca przechowywania, rejestracja wypożyczeń),
- okresowe wykonywanie, przechowywanie i sprawdzanie kopii zapasowych informacji zgodnie z zasadami tworzenia kopii.

Klasyfikacja informacji

Klasyfikacja informacji została przeprowadzona na podstawie wykazu aktywów informacyjnych, uwzględnionych w analizie ryzyka. Rodzaj informacji odpowiada rodzajom aktywów informacyjnych. W analizie ryzyka podane są zasoby, na których znajdują się informacje należące do poszczególnych rodzajów. Ogólna klasyfikacja informacji chronionych dzieli je na dwie zasadnicze grupy: informacje własne i informacje klienta.

W tabelach poniżej dla każdego rodzaju informacji podane zostały dokumenty określające zasady postępowania oraz lokalizacja informacji chronionych.

Informacje własne

Klasa informacji	Rodzaj informacji	Zasady postępowania w zakresie bezpieczeństwa	Obszar odpowiedzialny za ochronę
Dane osobowe	Dane osobowe pracowników	Ustawa o ochronie danych osobowych, Polityka ochrony danych osobowych, Polityka bezpieczeństwa informacji	Administrator Danych
Tajemnica WIML	Dane finansowo - księgowe	Ustawa o rachunkowości, Polityka bezpieczeństwa informacji	Właściciel aktywa
	Dane i informacje powierzone przez klientów	Polityka bezpieczeństwa informacji, Umowy z innymi podmiotami, Regulamin	Właściciele aktywów
	Dane klientów	Polityka bezpieczeństwa informacji	Właściciel aktywa
	Dane osobowe klientów / pacjentów	Polityka ochrony danych osobowych Umowy powierzenia	Administrator Danych
	Umowy	Polityka bezpieczeństwa informacji	Właściciel aktywa
	Dokumentacja ofertowa	Polityka bezpieczeństwa informacji, ustawa pzp	Właściciel aktywa
	Dokumentacja operacyjna	Nadzór nad dokumentami i zapisami, Polityka bezpieczeństwa informacji	Właściciel aktywa
	Dokumentacja techniczna urządzeń	Gospodarka konserwacyjno-remontowa, Polityka bezpieczeństwa informacji	Właściciel aktywa
	Część dokumentacji ZSZ	Nadzorowanie zapisów, Polityka bezpieczeństwa informacji	Pełnomocnik ZSZ
	Hasła do systemów i sieci	Polityka kontroli dostępu do systemów i sieci	Użytkownicy
Informacje publiczne	Dokumentacja przetargowa po rozstrzygnięciu przetargów, informacje handlowe	Nadzorowanie zapisów, Polityka bezpieczeństwa informacji	Pracownicy WIML

W celu zapobiegania nieautoryzowanemu dostępowi oraz naruszeniu bezpieczeństwa lub kradzieży informacji i środków jej przetwarzania prowadzona jest polityka czystego biurka i czystego ekranu.

Polityka czystego biurka

Ważne dokumenty i nośniki danych nie powinny pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pokoju. Pokój należy zamknąć na klucz. Po zakończeniu pracy ważne dokumenty i komputerowe nośniki z danymi powinny być przechowywane w zamkniętych szafach, pokoje zamknięte na klucz.

Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników. Pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenie zleconego zadania. Nie powinny one pozostawać dostępne ani dla obcych osób ani dla pracowników nie posiadających stosownych uprawnień.

Polityka czystego ekranu

Zasada „czystego ekranu" odnosi się do serwerów, stacji roboczych, terminali komputerowych oraz urządzeń przenośnych — laptopów, palmtopów, tabletów itp. Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone wylogowaniem się lub zablokowaniem klawiatury i włączeniem wygaszacza ekranu zabezpieczonego hasłem. Czynność ta może odbywać się automatycznie, pod warunkiem, że **czas aktywacji zabezpieczenia** jest wystarczająco krótki i wynosi **maksymalnie 20 minut**.

Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wyrejestrować się (wylogować się) z serwerów lub też stosować oprogramowanie blokujące klawiaturę i wygaszacz ekranu zabezpieczony hasłem.

W związku z użytkowaniem komputerów stacjonarnych wprowadza się następujące zasady:

- zabrania się korzystania ze stanowisk komputerowych w celach niezwiązanych z interesem WIML.
- dostęp do systemu operacyjnego komputera powinien być zabezpieczony hasłem.
- wprowadza się obowiązek korzystania tylko z przypisanych danemu pracownikowi komputerów, a jeśli nie jest to możliwe, korzystanie z innych komputerów, ale zawsze z własnym identyfikatorem i hasłem.
- zabrania się korzystania z aplikacji i systemów nie pod swoim loginem i hasłem.
- opuszczenie stanowiska pracy, któremu towarzyszy wyjście z pomieszczenia, musi zakończyć się zablokowaniem komputera lub włączeniem wygaszacza ekranu zabezpieczonego hasłem. Włączenie wygaszacza ekranu zabezpieczonego hasłem nie musi wymagać wykonania odpowiedniego działania ze strony użytkownika, może odbywać się automatycznie, pod warunkiem, że czas aktywacji zabezpieczenia jest wystarczająco krótki (**maksymalnie. 20 minut**).
- stosowanie zaleceń administratora w zakresie uaktualniania programów antywirusowych zainstalowanych na komputerach WIML.

- pracownicy wprowadzający informacje do systemów informatycznych powinni dokonywać sprawdzenia poprawności wprowadzanych danych.
- z WIML nie wolno wynosić sprzętu komputerowego (ani jego składników) bez zezwolenia przełożonego.

Do mobilnych środków przetwarzania i komunikacji zalicza się m.in. komputery przenośne, palmtopy, tablety itp. oraz telefony komórkowe. Przez wzgląd na bezpieczeństwo informacji zgromadzonych na mobilnych środkach wprowadza się następujące zasady:

- zabrania się przechowywania danych osobowych w pamięci lub na dyskach mobilnych środków przetwarzania i komunikacji.
- urządzenia mobilne będące własnością WIML, są przypisane konkretnemu pracownikowi, osoba przypisana do urządzenia mobilnego odpowiada za jego bezpieczeństwo (kradzież, utrata lub ujawnienie danych),
- zabrania się pracownikom WIML, korzystania z środków mobilnych, a w szczególności z komputerów przenośnych w celach niezwiązanych ściśle z interesem WIML.
- wynoszenie komputerów przenośnych poza teren WIML, musi być uzgodnione z przełożonym. Zaleca się zachowanie szczególnej ostrożności podczas używania tych urządzeń poza siedzibą WIML, a zwłaszcza w miejscach publicznych.
- urządzenie mobilne powinno być zabezpieczone hasłem dostępu do systemu operacyjnego lub blokadą klawiatury (telefony komórkowe).
- wymagane jest wykonywanie odpowiednich kopii zapasowych znaczących informacji. przechowywanych w urządzeniu mobilnym, aby w przypadku utraty lub uszkodzenia urządzenia możliwe było ich odtworzenie.
- podłączając urządzenie mobilne do Internetu lub innej sieci informatycznej poza siedzibą WIML należy zapewnić jego ochronę przed złośliwym i szkodliwym oprogramowaniem.
- stosowanie zasady „czystego ekranu”. W przypadku odejścia od komputera przenośnego powinno zostać poprzedzone włączeniem wygaszacza ekranu zabezpieczonego hasłem z zachowaniem wyżej opisanych wymagań.
- urządzenia mobilne nie powinny być pozostawiane w miejscach publicznych oraz w samochodzie bez nadzoru.
- pracownik odpowiada za nieautoryzowany dostęp osób nieupoważnionych do danych zawartych w swoim urządzeniu mobilnym.
- w razie zagubienia lub kradzieży komputera przenośnego użytkownik zobowiązany jest do niezwłocznego działania zgodnie z polityką zarządzania incydentami.

Zarządzanie incydentami

Zdarzenie – jest to określony stan systemu, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

Incydent - jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które znacznie zwiększają prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

W WIML, przyjmuje się następujące zakresy rejestrowania incydentów:

- naruszenie polityki bezpieczeństwa informacji w WIML: informacji dotyczących WIML, informacji dotyczących Klientów,
- naruszenie obowiązujących polityk i zasad,
- wykryte próby lub faktyczne: włamania, napaści, kradzieży, włamania do systemu IT, podszycia się pod użytkownika konta informatycznego,
- interwencje ochrony,
- sytuacje pożarowe,
- załączenia systemów alarmowych,
- awarie: systemów WIML, maszyn niszczących,
- fakty posiadania niedostatecznych umiejętności użytkowników, przekroczenia uprawnień, niedopełnienia obowiązków, zaniedbań.
- fakty wydostania się nośników informacji lub pochodzących od nich informacji do miejsc niepożądanych.

O ile to możliwe, osoba stwierdzająca wystąpienie incydentu niezwłocznie podejmuje działania mające na celu niedopuszczenie lub usunięcie skutków naruszenia polityki bezpieczeństwa w WIML.

Stwierdzenie incydentu zgłaszane jest Pełnomocnikowi ds. ZSZ. Stwierdzenie zagrożenia danych osobowych zgłaszane jest bezzwłocznie dodatkowo Inspektorowi Ochrony Danych.

Zgłaszane incydenty rejestrowane są przez Pełnomocnika ds. ZSZ. Rejestr jest należycie chroniony przed dostępem osób niepowołanych.

Zarejestrowane incydenty stanowią podstawę do oceny skuteczność zabezpieczeń i omawiane są na przeglądzie systemu.

Każdemu wykrytemu incydentowi musi być przypisany właściwy dla niego poziom zagrożenia - dalszy proces postępowania uzależniony jest ściśle od przypisanego poziomu. Poziom zagrożenia określa Pełnomocnik ds. ZSZ, a w przypadku danych osobowych Inspektor Ochrony Danych.

Odnotowanie incydentu zawiera:

– datę i godzinę wystąpienia, miejsce wystąpienia incydentu, opis incydentu, osoby związane z incydentem, opis działań po incydencie.

Ze względu wpływu na bezpieczeństwo informacji przyjęto poniższy podział incydentów:

– **Krytyczny** – utrata poufności, integralności lub dostępności informacji klienta, danych osobowych, własnej informacji chronionej, poważne naruszenie obowiązków pracowniczych, włamanie, napaść, kradzież, pożar itp.

– **Ważny –** pojedyncze przypadki: nie wypełniania obowiązków, wymagań polityk bezpieczeństwa informacji lub zasad, które mogą w rezultacie doprowadzić do incydentu krytycznego.

Postępowanie w przypadku zaistnienia zdarzenia o określonym poziomie zagrożenia:

– **Krytyczny** – w przypadku wystąpienia incydentu kwalifikującego się do poziomu „Krytyczny" wyciągane są konsekwencje służbowe, lub prawne w stosunku do osób, które przyczyniły się do wystąpienia incydentu. Dopuszcza się możliwość wezwania odpowiednich służb: policji, żandarmerii wojskowej, straży miejskiej lub straży pożarnej. W przypadku zagrożenia danych osobowych Inspektor Ochrony Danych informuje o fakcie Prezesa Urzędu Ochrony Danych (czas do 72 godzin od momentu wystąpienia incydentu).
Ważny – w przypadku wystąpienia incydentu kwalifikującego się do poziomu „Ważny" Pełnomocnik ds. ZSZ, po ewentualnym uzgodnieniu decyzji z Inspektorem Ochrony Danych, wnioskuje o przeprowadzenie rozmowy pouczającej z osobami odpowiedzialnymi za wystąpienie incydentu lub organizuje spotkanie w celu wyjaśnienia zajścia incydentu.

Analiza incydentu i raportowanie

Incydent zakwalifikowany jako „**Krytyczny**" inicjuje działania, zgodnie z procedurą *Działania korygujące i doskonalące* , dokumentując następujące informacje:

– przyczynę i okoliczności zaistnienia incydentu,

– osoby odpowiedzialne za obsługę incydentu,

– przebieg zdarzenia i podjęte działania,

– efekt przeprowadzonych działań,

– wpływ na bezpieczeństwo przetwarzanych informacji,

– sprawcy zdarzenia i ewentualne konsekwencje wynikające z analizy incydentu.

Obsługa zdarzenia kwalifikującego się do poziomu „Ważny" powinna zakończyć się:

– analizą przyczyn incydentu i częstotliwości jego występowania,

– jeżeli częstotliwość występowania jest duża, wówczas należy postępować jak z incydentem zaklasyfikowanym jako „Krytyczny”.

Zgodność

Dla zapewnienia zgodnego z prawem działania w WIML przepisy prawa, w poszczególnych obszarach, są identyfikowane, aktualizowane i okresowo przeglądane (nie rzadziej niż raz w roku). Wyniki zapisane są w *Rejestrze wymagań prawnych i innych* (formularz F-ZSZ-16*).*

Metodyka szacowania ryzyka

Opis metodyki szacowania ryzyka jest zawarty w dokumencie „Metodyka szacowania ryzyka”

Jako **kryterium** wyznaczania **poziomu akceptacji ryzyka** jest dążenie do wyrównania ryzyk szczątkowych aktywów w WIML. Wartość **ryzyka akceptowalnego** jest każdorazowo ustalana na przeglądach zarządzania.

Wykaz zmian

Lp.	Data zmiany	Nr strony	Krótki opis zmiany	Wprowadził
Wykaz zmian w wydaniu 4.0				
	24.07.2018 r.	3	dodano zapisy o danych osobowych (4wg, 3wd)	M. Dereń
	24.07.2018 r.	3	wpisano: Administrator Systemu Informatycznego odpowiada za: (6wd)	M. Dereń
	24.07.2018 r.	4	wpisano: : Administrator Systemu Informatycznego…, Inspektor Ochrony Danych… (17-18wd)	M. Dereń
	24.07.2018 r.	6	wpisano: : Inspektor Ochrony Danych (w przypadku danych osobowych)	M. Dereń
	24.07.2018 r.	15	dodano wiersz „Dane osobowe klientów / pacjentów ….(8wgt)	M. Dereń
	24.07.2018 r.	18	dodano: podszycia się użytkownika konta informatycznego (24wd)	M. Dereń
	24.07.2018 r.	18	dodano: „Stwierdzenie zagrożenia … Danych” (12wd)	M. Dereń
	24.07.2018 r.	19	dodano: „…danych osobowych..” (4wg)	M. Dereń
	24.07.2018 r.	19	dodano: „…po ewentualnym uzgodnieniu decyzji z Inspektorem Ochrony Danych.” (15wd)	M. Dereń
Wykaz zmian w wydaniu 4.1				