Instrukcja nr 3 do Polityki
bezpieczeństwa danych w
systemach informacyjnych.

Instrukcja
Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka

WSTĘP

Środki, jakie administrator danych zobowiązany jest zastosować, powinny być odpowiednie do zakresu, kontekstu i celu, a także ryzyka naruszenia ochrony przetwarzanych danych.
Przyjęte rozwiązania określają jakie środki bezpieczeństwa należy zastosować w celu minimalizacji ryzyka zaistnienia zagrożenia dla danych osobowych przetwarzanych w systemie informatycznym.
Określamy środki jakie zastosujemy ustanawiając zabezpieczenia minimalizujących to ryzyko uwzględniamy stan wiedzy technicznej, koszt wdrażania, a także skutki, jakie urzeczywistnienie się zidentyfikowanych zagrożeń może powodować dla osób, których dane są przetwarzane.
Zgodnie z art. 32 RODO na potrzeby zapewnienia właściwego bezpieczeństwa, wdrażamy odpowiednie środki techniczne i organizacyjne, w tym takie jak:

- pseudonimizacja i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Administrator Danych stosuje dostępne środki bezpieczeństwa mając na względzie między innymi fakt, że systemy używane do przetwarzania danych połączone zostały z siecią wykorzystywaną do świadczenia usług publicznych, z której mogą pochodzić dodatkowe zagrożenia (Internet).

ROZDZIAŁ 1 Postanowienia ogólne

Instrukcja Zarządzania Systemami Informatycznymi jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania Systemami Informatycznymi Instytutu Matki i Dziecka. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych w systemach informatycznych, w szczególności zaś osoby pełniące funkcje:

1. Inspektora Ochrony Danych (IOD) w Instytucie Matki i Dziecka.
2. Zastępcę Inspektora Ochrony Danych (ZIOD) w Instytucie Matki i Dziecka.
3. Kierowników jednostek i komórek organizacyjnych Instytutu Matki i Dziecka.
4. Administratora Systemów Informatycznych (ASI) wyznaczonego w Instytucie Matki i Dziecka.
5. Inne osoby wskazane przez Administratora Danych, w tym osoby, które są podmiotami zewnętrznymi współpracującymi z Instytutem Matki i Dziecka biorącymi udział w procesie przetwarzania danych.

ROZDZIAŁ 2 Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych

§ 1

1. Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych zapoznaje się z:
   a. Niniejszą instrukcją.
   b. Procedurami określonymi przez Administratora Danych.
2. Podstawą nadania uprawnień jest wniosek kierownika jednostki lub komórki organizacyjnej zawarty w Załączniku nr 4 do Instrukcji Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka.

§ 2

Opis procedury nadawania/odbierania uprawnień dostępu do lokalnej sieci komputerowej przedstawiony jest poniżej. W Instytucie Matki i Dziecka użytkownicy uzyskują dostęp do sieci komputerowej i systemów informatycznych na z góry zdefiniowanym poziomie uprawnień w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku. **Postępowanie:**

1. Kierownik jednostki/komórki organizacyjnej:
   a. Wnioskuje o nadanie/modyfikację/odebranie pracownikowi uprawnień do przetwarzania danych w systemach/aplikacjach eksploatowanych w sieci komputerowej, Instytutu Matki i Dziecka w związku z wykonywanymi przez niego zadaniami.
   b. Zgłasza do ASI potrzebę nadania/modyfikacji/odebrania uprawnień w systemie informatycznym na wymaganym poziomie, na formularzu stanowiącym Załącznik nr 4 do „Instrukcji Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka”.
2. ASI na podstawie otrzymanego formularza, wykonuje:
   a. Rejestruje/usuwa użytkownika w systemie i nadaje lub odbiera mu wymagane uprawnienia.
   b. Informuje Kierownika jednostki lub komórki organizacyjnej w formie elektronicznej oraz IOD o fakcie nadania/odebrania uprawnień. W przypadku nadania uprawnień, informuje dodatkowo użytkownika o nadanych uprawnieniach oraz sposobie dostępu do systemu informatycznego.
   c. W przypadku, gdy nadanie pracownikowi wymaganych uprawnień może grozić naruszeniem standardów bezpieczeństwa systemów informatycznych pracujących w sieci, ASI informuje przełożonego użytkownika oraz IOD w formie elektronicznej o tym zagrożeniu i wstrzymuje proces nadawania uprawnień. Przełożony użytkownika ponownie może wnioskować o przyznanie pracownikowi zmodyfikowanych uprawnień, które nie stanowią zagrożenia naruszenia bezpieczeństwa, a jego wniosek musi zostać zaakceptowany przez IOD.
3. Użytkownik, po otrzymaniu od ASI informacji o założonym koncie z wymaganymi uprawnieniami, wykonuje:
   a. logowanie do systemu informatycznego w celu sprawdzenia poprawności konta i uprawnień.
   b. przy pierwszym logowaniu się do systemu informatycznego, użytkownik musi zmienić nadane mu przez ASI hasło.
4. Powyższy schemat nadania/odebrania uprawnień dostępu do systemów informatycznych eksploatowanych w sieci komputerowej należy stosować również w przypadku wymaganej zmiany w istniejących uprawnieniach użytkownika.

§ 3

5. Powyższe zasady nadawania/modyfikacji/odbierania uprawnień dostępu do wszystkich systemów informatycznych eksploatowanych w Instytucie Matki i Dziecka obowiązują wszystkich pracowników, jak również osoby i firmy współpracujące z IMiD.
6. W przypadku, gdy system informatyczny nie posiada wbudowanych mechanizmów kontroli dostępu, wówczas należy niezwłocznie rozbudować taki system o te mechanizmy, a do czasu wdrożenia takich mechanizmów należy zaimplementować ograniczenia dostępu na poziomie systemu operacyjnego, bądź ograniczenia proceduralne.

ROZDZIAŁ 3 Metody i środki uwierzytelnienia w systemach informatycznych

§ 1

1. Naczelną zasadą bezpieczeństwa systemów informatycznych i sieci komputerowej jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników systemów informatycznych (w tym sieci komputerowej) ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 2

1. W systemach informatycznych Instytutu Matki i Dziecka stosuje się uwierzytelnienie dwustopniowe, na poziomie:
   a. Dostępu do sieci komputerowej lub sprzętu komputerowego.
   b. Dostępu do systemu informatycznego.
2. Do uwierzytelnienia użytkownika w systemie informatycznym na obu poziomach używa się identyfikatorów, haseł lub karty inteligentnej.
   a. Stosowanie unikalnych identyfikatorów użytkownika oraz haseł zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach i sieciach teleinformatycznych Instytutu Matki i Dziecka.
   b. Zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi (nie dopuszcza się, aby użytkownik korzystał z kont: administrator, gość, a także z konta innego użytkownika).
   c. Ograniczenie dostępu do informacji jedynie do kręgu użytkowników uprawnionych (autoryzowanych) wymaga przyjęcia odpowiednio dobranej polityki stosowania haseł.
3. W Instytucie Matki i Dziecka, stosuje się poziom bezpieczeństwa przetwarzania danych adekwatny do klasyfikacji tych danych w systemach informatycznych. W związku z powyższym, ustala się wysoki poziom bezpieczeństwa, który jest przeznaczony dla systemów informatycznych, w których są przetwarzane dane wrażliwe oraz co najmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych jest połączone z siecią publiczną.
4. Hasło dostępu do sieci komputerowej, systemu informatycznego musi składać się z minimum 8 znaków zawierających duże i małe litery cyfry i znaki.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych słów bezpośrednio kojarzących się z użytkownikiem.
6. Hasło nie może być ujawnione innej osobie nawet po utracie ważności hasła.
7. System automatycznie powinien wymuszać zmianę hasła nie rzadziej, niż jeden raz w miesiącu. Hasło musi być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia.
8. Obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu, oraz przekazywania tych haseł osobom trzecim.

§ 3

Procedura zarządzania środkami uwierzytelniania:

   a. ASI nadaje hasło dostępu do systemu informatycznego lub sieci komputerowej dla nowego użytkownika albo dla użytkownika, który zapomniał swojego ostatniego hasła.
   b. Użytkownik systemu informatycznego niezwłocznie, po nadaniu hasła przez ASI, ustala swoje, znane tylko jemu hasło. System automatycznie wymusza na użytkowniku zmianę nadanego przez administratora hasła przy pierwszym logowaniu.
   c. Użytkownik systemu w dowolnym momencie może zmienić swoje hasło dostępu do systemu informatycznego.
   d. Obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu.
   e. ASI zapisuje swój identyfikator oraz hasła dostępu po każdej ich zmianie i umieszcza je w kopercie, a następnie przekazuje zamkniętą kopertę do przechowania w wyznaczonej do tego celu szafie metalowej ulokowanej w pomieszczeniach Działu Informatyki lub Kancelarii. Koperta taka może być awaryjnie udostępniona innemu administratorowi za zgodą przełożonego ASI. Przełożony ASI odpowiedzialny jest za prowadzenie rejestru udostępnionych awaryjnie haseł. Po awaryjnym użyciu hasła, musi ono zostać jak najszybciej zmienione przez ASI.

ROZDZIAŁ 4 Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

§ 1

Procedura rozpoczęcia pracy:

a. Uruchomić komputer wchodzący w skład systemu informatycznego, zalogować się podając własny identyfikator i hasło dostępu.
b. Jeśli użytkownik wprowadzi 3-krotnie błędnie hasło, wówczas jego identyfikator i hasło może zostać zablokowane. W celu odblokowania swojego identyfikatora, użytkownik postępuje według procedury obowiązującej przy nadawaniu/odbieraniu uprawnień dostępu do systemów informatycznych opisanej w Rozdziale 2, § 2.
c. Uruchomić wybrany system/aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane).
d. Zalogować się do systemu/aplikacji podając własny identyfikator i hasło dostępu.
e. Jeśli użytkownik wprowadzi 3-krotnie błędnie hasło, wówczas jego identyfikator i hasło może zostać zablokowane. W celu odblokowania swojego identyfikatora, użytkownik postępuje według procedury obowiązującej przy nadawaniu/odbieraniu uprawnień dostępu do systemów informatycznych opisanej w Rozdziale 2, § 2.

Procedura zawieszenia pracy w systemie/aplikacji:

1. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy poprzez zablokowanie komputera, zamknięcie systemu/aplikacji spowodować, aby na ekranie nie były wyświetlane informacje lub dane.
2. Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem lub wylogowania się z systemu.

Procedura zakończenia pracy w systemie:

a. Zamknąć system/aplikację.
b. Zamknąć system operacyjny komputera i poczekać na jego wyłączenie.
c. Wyłączyć monitor.
d. Sprawdzić, czy elektroniczne nośniki informacji zawierające dane nie zostały pozostawione bez nadzoru.

4. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia się ze sprzętu komputerowego.

ROZDZIAŁ 5 Procedury tworzenia kopii zapasowych danych

§ 1

1. W celu zapewnienia optymalnego poziomu ochrony danych przetwarzanych w systemach informatycznych Instytutu Matki i Dziecka, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach danych Instytutu Matki i Dziecka w oparciu o architekturę klient – serwer. Wynika stąd praktyka przetwarzania danych w bazach danych na dedykowanych dla systemu/aplikacji serwerach.
2. Jeśli stosowane dotychczas rozwiązania nie są zgodne z architekturą klient – serwer, to należy zapewnić możliwość przechowywania gromadzonych za ich pomocą danych na wyznaczonym serwerze plików.
3. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Instytutu Matki i Dziecka, stanowią jedynie końcówki klienckie systemu komputerowego.

4. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach sieciowych aplikacji bazodanowych są zapisywane bezpośrednio na serwerach.
5. W szczególnych przypadkach, za zgodą IOD, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych niepodłączonych do sieci komputerowej Instytutu Matki i Dziecka. W takich przypadkach obowiązek wykonania kopii bezpieczeństwa aplikacji oraz codziennego wykonywania kopii bezpieczeństwa bazy danych oraz ich bezpiecznego przechowywania (zgodnie z zasadami opisanymi w poniższym § 2 pkt.3), spoczywa bezpośrednio na użytkowniku danej aplikacji.
6. Opisywana tu zasada przetwarzania danych wpływa bezpośrednio na zagadnienia związane z tworzeniem kopii bezpieczeństwa systemów.

§ 2

1. Kopie zapasowe danych, baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są (…) zgodnie z zasadami określonymi w instrukcji systemu tworzenia kopii zapasowych.

(…)

ROZDZIAŁ 6 Przechowywanie nośników informacji zawierające dane oraz kopii zapasowych § 1 Elektroniczne nośniki informacji

1. Dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (…),które są własnością Instytutu Matki i Dziecka w Warszawie.

ROZDZIAŁ 7 Środki ochrony systemów informatycznych

§ 1

Poniżej przedstawiono zasady ochrony systemów przetwarzania danych przed „szkodliwym oprogramowaniem” oraz próbami penetracji przez osoby nieuprawnione.

1. Ochrona antywirusowa:
   a. Za ochronę antywirusową odpowiada ASI.
   b. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego.
   c. Oprogramowanie antywirusowe jest instalowane centralnie na serwerze, oraz na wszystkich stanowiskach komputerowych podłączonych do sieci.

   (…)

   Użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.

§ 2

1. ASI jest odpowiedzialny za aktywowanie i poprawną konfigurację specjalistycznego oprogramowania monitorującego wymianę danych na połączeniu:
   a. Sieci lokalnej i sieci rozległej.
   b. Stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
2. ASI obowiązany jest do utrzymywania stałej aktywności zainstalowanego specjalistycznego oprogramowania monitorującego wymianę danych oraz do jego aktualizacji.
3. Ochrona przed awarią zasilania:

a. System, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

(…)

ROZDZIAŁ 8 Monitorowanie dostępu do danych

§ 1

1. Dla każdego systemu, w którym przetwarzane są dane osobowe, prowadzona jest ewidencja, w której odnotowywane są informacje o odbiorcach danych z tego systemu (o ile występuje dla danego systemu proces udostępniania danych osobom wymienionym w rozdziale 8 § 1 pkt.2).
2. Każdy wniosek o udostępnienie danych osobowych powinien zostać zgłoszony do IOD.
3. Odbiorca oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. Strona trzecia oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
4. Odnotowanie obejmuje informacje o:
   a. Nazwie jednostki, komórki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane.
   b. Zakresie udostępnianych danych.
   c. Dacie udostępnienia.
5. Obowiązek odnotowania ww. informacji w Ewidencji spoczywa na użytkowniku systemu udostępniającemu dane.
6. Odnotowanie informacji w Ewidencji powinno nastąpić niezwłocznie po udostępnieniu danych.
7. Udostępnienie danych osobowych może nastąpić w przypadkach opisanych w art. 6 lub 9 RODO.
8. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
9. Nadzór nad prawidłowością odnotowywania w Ewidencji ww. informacji sprawuje IOD.

ROZDZIAŁ 9 Procedury wykonywania przeglądów i konserwacji systemu

§ 1

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 ASI.
   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.

§ 2

1. Przegląd systemów/aplikacji i narzędzi programistycznych przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach: a. Zmiany wersji oprogramowania systemu/aplikacji.
   b. Zmiany wersji oprogramowania na stanowisku komputerowym użytkownika.
   c. Zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowany jest system/aplikacja.
   d. Zmiany systemu operacyjnego na stanowisku komputerowym użytkownika.
   e. Wykonania zmian w systemie/aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu.

(…)

2. Za prawidłowość przeprowadzenia procesu przeglądu i konserwacji systemu/aplikacji odpowiada przełożony ASI lub inny wyznaczony pracownik Działu Informatyki.

§ 3

Konserwacja systemów/aplikacji wykorzystywanych przez użytkowników.

1. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu/aplikacji potrzeby wprowadzenia zmian pozwalających dostosować funkcjonalność systemu/aplikacji do obsługi bieżących i planowanych potrzeb Instytutu Matki i Dziecka. Zgłoszenie kierowane jest do Działu Informatyki.

(…)

Załączniki do Instrukcji:

1. Załącznik nr 1 - Regulamin korzystania z sieci komputerowej przez pracowników w Instytucie Matki i Dziecka.
2. Załącznik nr 2 - Zasady użytkowania sprzętu komputerowego przez pracowników w Instytucie Matki i Dziecka.
3. Załącznik nr 3 - Zasady udzielania pomocy użytkownikom sprzętu komputerowego w Instytucie Matki i Dziecka.
4. Załącznik nr 4 - Wniosek przełożonego o nadanie uprawnień dla użytkowników w systemie informatycznym.
5. Załącznik nr 5 - Rejestr kopii zapasowych.

Załącznik nr 1
Do Instrukcji Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka

Regulamin
korzystania z Sieci Komputerowej przez pracowników Instytutu Matki i Dziecka.

§ 1

1. Regulamin ustala zasady korzystania z sieci komputerowej Instytutu Matki i Dziecka przez pracowników Instytutu Matki i Dziecka.

2. Dokumentami nadrzędnymi w stosunku do niniejszego regulaminu jest „Instrukcja Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka” oraz „Polityka bezpieczeństwa danych w systemach informacyjnych”.

§ 2

1. Sieć Komputerową Instytutu Matki i Dziecka tworzą:
   a. Sieć lokalna Instytutu Matki i Dziecka.
   b. Ogólno-instytutowe serwery kont i usług sieciowych.
2. Funkcję ASI Instytutu Matki i Dziecka pełni osoba wyznaczona zarządzeniem Administratora Danych przez Kierownika Działu Informatyki.

§ 3

1. Użytkownikiem systemu w Instytucie Matki i Dziecka jest każda osoba korzystająca z komputera bądź terminala podłączonego do sieci komputerowej Instytutu.
2. Konto użytkownika systemu/aplikacji to zarejestrowane uprawnienie do pracy na jednym z serwerów w sieci komputerowej Instytutu Matki i Dziecka.
3. Konta na serwerze są przydzielane wszystkim pracownikom Instytutu Matki i Dziecka zgodnie z ustaloną procedurą:
   a. Przełożony pracownika zgłasza potrzebę założenia konta dla nowego pracownika zgodnie z wnioskiem stanowiącym załącznik nr 4a/4b do Instrukcji Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka w zależności od koniecznych uprawnień.
   b. Konto użytkownika systemu daje uprawnienia do korzystania z poczty elektronicznej i innych usług sieciowych Instytutu Matki i Dziecka wymagających uwierzytelnienia. W uzasadnionych przypadkach na wniosek przełożonego użytkownika, ASI może zmienić uprawnienia konta.
4. ASI określa warunki techniczne i organizacyjne korzystania z kont oraz ograniczenia rozmiaru zużywanej przestrzeni dyskowej.
5. Pracownicy Instytutu Matki i Dziecka korzystają z poczty poprzez wskazanego przez ASI klienta serwera pocztowego lub dowolną przeglądarkę internetową.
6. Przesyłanie i odbieranie korespondencji służbowej odbywa się poprzez służbowe skrzynki pocztowe.
7. Pojemność skrzynek pocztowych pracowników Instytutu Matki i Dziecka jest ograniczona. Po przekroczeniu tej wartości zostanie zablokowana możliwość wysyłania wiadomości do momentu oczyszczenia skrzynki pocztowej. W uzasadnionych przypadkach na wniosek przełożonego użytkownika, ASI może zwiększyć wielkość skrzynki.
8. Pracownicy mają możliwość przechowywania swojej poczty na stacjach roboczych, wiąże się to jednak z tym, że pełna odpowiedzialność za ewentualną utratę danych jest po stronie użytkownika systemu.
9. Dział Kadr i Płac przekazuje dane dotyczące rozwiązania/zawarcia umowy o pracę z pracownikami Instytutu Matki i Dziecka do Działu Informatyki.
10. W przypadku pracownika, z którym został rozwiązany stosunek pracy, ASI zobowiązany jest zarchiwizować dane tego użytkownika systemu, wyłączyć konta a po upływnie 6 miesięcy skasować konta wraz z uprawnieniami.
11. Konta pracowników, którzy pozostają w stosunku pracy, ale utracili uprawnienia do ich posiadania są kasowane po upływie 2 miesięcy.

§ 4

1. Każdy użytkownik systemu Instytutu Matki i Dziecka powinien postępować zgodnie z powierzonymi mu obowiązkami, a w szczególności z poniższymi zasadami:
   a. Używanie poczty elektronicznej tylko do celów służbowych.
   b. Korzystanie z Internetu tylko do celów służbowych.
   c. Korzystanie z systemów/aplikacji Instytutu Matki i Dziecka tylko do celów służbowych.
2. Zabronione jest:

a. Wysyłanie masowej poczty kierowanej do losowych odbiorców (spam).
b. Ściąganie i udostępnianie treści chronionych prawem autorskim (filmy, utwory muzyczne, oprogramowanie).
c. Udostępnianie treści zakazanych (np. pornografia).
d. Nieuzasadnione wynoszenie danych zawartych na nośnikach poza Instytutem Matki i Dziecka.

3. Pracodawca zastrzega sobie prawo do monitorowania ruchu w sieci LAN Instytutu Matki i Dziecka, w zakresie określonym w powyższych ust. 1 i 2.
4. Jeżeli zaistnieje potrzeba podłączenia komputera prywatnego (laptop) pracownika do sieci LAN Instytutu Matki i Dziecka, wymaga to wykonania następujących czynności:
   a. Napisania wniosku o podłączenie wraz z uzasadnieniem.
   b. Akceptacji wniosku przez przełożonego pracownika.
   c. Akceptacji wniosku przez Kierownika Działu Informatyki.
4. Zabrania się podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci.
5. Zabrania się uruchamiania aplikacji, które mogą zakłócić i destabilizować pracę systemu lub sieci komputerowej, bądź naruszyć prywatność zasobów systemowych.
6. W przypadku naruszenia zasad opisanych w ust. 1 ASI rejestruje incydent, blokuje dostęp do konta użytkownika. Powiadamiana o tym fakcie Inspektora Ochrony Danych oraz przełożonego pracownika.
7. W przypadku stwierdzenia, że komputer dołączony do sieci LAN generuje strumień danych zakłócający pracę sieci lub wskazujący na używanie tego komputera jako niezarejestrowanego serwera danych, ASI ma prawo zablokować dostęp do tego komputera do czasu wyjaśnienia sprawy. Rejestruje incydent i powiadamia o zaistniałej sytuacji Inspektora Ochrony Danych oraz przełożonego pracownika.

Załącznik nr 2
Do Instrukcji Zarządzania Systemami Informatycznymi w
Instytucie Matki i Dziecka

Zasady

użytkowania sprzętu komputerowego przez pracowników Instytutu Matki i Dziecka.

§ 1.

Zasady użytkowania sprzętu komputerowego przez pracowników Instytutu Matki i Dziecka, zwane dalej zasadami, określają prawa i obowiązki użytkowników sprzętu komputerowego.

§ 2.

Ilekroć w zasadach jest mowa o:

1. **Helpdesk** - rozumie się przez to pracowników Działu Informatyki przyjmujących i realizujących zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania komputerowego.
2. **Sprzęcie komputerowym** - rozumie się przez to komputer oraz urządzenia peryferyjne, w tym: monitor, drukarka, skaner, terminal, konsole itp. wymagające do swojego działania połączenia z komputerem.
3. **Nośniki elektroniczne** - urządzenia umożliwiające zapisywanie i przenoszenie danych (np. dyskietka, twardy dysk, płyta CD, pamięci masowe, karty magnetyczne, pamięci USB - pendrive).

§ 3.

1. Użytkownikowi systemu przysługuje prawo:
   a. Do korzystania ze sprzętu komputerowego i sieci komputerowej wyłącznie w zakresie powierzonych mu zadań.

b. Do korzystania z oprogramowania komputerowego zgodnie z umowami i ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj. Dz. U. z 2021 r., poz. 1062).

§ 4.

Informacje zapisane na nośnikach elektronicznych należą do pracodawcy – Instytutu Matki i Dziecka.

§ 5. O przekazaniu sprzętu komputerowego użytkownikowi decyduje przełożony użytkownika.

§ 6. Użytkownik jest materialnie odpowiedzialny za sprzęt komputerowy, który otrzymał do wykonywania obowiązków służbowych.

§ 7.

Dział Informatyki prowadzi sprawy w zakresie użytkowania sprzętu komputerowego i oprogramowania komputerowego, a w szczególności:

a. Sprawuje nadzór nad wykonaniem umów, dotyczących zakupu/serwisu sprzętu i oprogramowania.
b. Prowadzi ewidencję sprzętu i oprogramowania.
c. Zabezpiecza sprawne działanie sprzętu komputerowego i oprogramowania.
d. Zapewnia standardy sprzętu komputerowego i oprogramowania spełniające wymagania Instytutu Matki i Dziecka.

§ 8.

1. W przypadku zmiany miejsca pracy użytkownika systemu na inną komórkę organizacyjną w Instytucie Matki i Dziecka, sprzęt komputerowy pozostaje w dotychczasowej komórce organizacyjnej.
2. Na przeniesienie sprzętu komputerowego wraz z użytkownikiem systemu do nowej komórki organizacyjnej musi wyrazić zgodę dotychczasowy przełożony użytkownika.
3. Użytkownik systemu jest zobowiązany do przekazania informacji do Działu Informatyki o przeniesieniu pracownika wraz ze sprzętem komputerowym do nowej komórki organizacyjnej.
4. Przełożony użytkownika zobowiązany jest do:
   a. Zlecenia Helpdesk zmiany lokalizacji sprzętu komputerowego.
   b. Informowania Helpdesk o przekazaniu sprzętu innemu użytkownikowi.

§ 9.

Każdy użytkownik systemu posiada identyfikator i hasło lub kartę inteligentną, które zabezpieczają dostęp do komputera, sieci komputerowej, urządzeń wielofunkcyjnych, baz danych i skrzynki pocztowej użytkownika.

§ 10. Zabronione jest:

a. Podłączanie przez użytkownika, bez zgody ASI, własnych urządzeń do sprzętu komputerowego lub sieci komputerowej**,**
b. Podłączania innych urządzeń niż informatyczne do wydzielonej sieci energetycznej do zasilania komputerów.
c. Samodzielnego instalowania oprogramowania.
d. Przemieszczenia sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany użytkownika bez uzgodnienia z Helpdesk.
e. Wynoszenie stacjonarnego sprzętu komputerowego poza teren Instytutu.
f. Fizyczne ingerowanie w konfigurację sprzętową urządzeń.
g. Samowolne odłączanie od sieci lub włącznie do sieci komputerowej sprzętu komputerowego.
h. Udostępnianie swojego identyfikatora i hasła do pracy innym osobom.
i. Pozyskiwanie informacji z komputerów innych użytkowników bez ich wiedzy.

j. Wykonywanie czynności, które mogą spowodować zakłócenia lub awarię sieci komputerowej.
k. Wynoszenie poza miejsce pracy nośników zawierających dane oraz przesyłanie niezabezpieczonych danych pocztą elektroniczną na zewnątrz.

§ 11.

1. Na stanowiskach pracy, na których używany jest sprzęt komputerowy obowiązują szczegółowe zasady jego użytkowania:
   a. Zakaz spożywania posiłków przy sprzęcie komputerowym.
   b. Zapewnienie warunków umożliwiających swobodne działanie układu chłodzenia użytkowanego sprzętu komputerowego.
   c. Utrzymanie czystości przy stanowiskach komputerowych.
   d. Zapewnienie odpowiedniego miejsca na lokalizację sprzętu komputerowego.
   e. Monitory komputerowe, na których przetwarzane są dane powinny być ustawione w ten sposób, aby osoby postronne znajdujące się w pomieszczeniu, jak i po zanim, ale posiadające środki fizyczne lub techniczne umożliwiające podgląd pomieszczenia nie miały możliwości zobaczenie, sfotografowania lub zapisania treści danych znajdujących się na ekranie.
   f. Zapewnienie odpowiednich mebli.
   g. Ustawienie z dala od źródeł wilgoci, grzejników lub innych substancji mogących zakłócić prawidłowe działanie sprzętu komputerowego.

Załącznik nr 3

Do Instrukcji Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka

Zasady

udzielania pomocy użytkownikom sprzętu komputerowego w Instytucie Matki i Dziecka.

§ 1.

1. Zasady udzielania pomocy użytkownikom sprzętu komputerowego w Instytucie Matki i Dziecka, zwane dalej zasadami, określają zasady postępowania w przypadku wystąpienia problemów w użytkowaniu sprzętu komputerowego lub zainstalowanego oprogramowania.
2. Dokumentem nadrzędnym w stosunku do niniejszych zasad jest procedura systemu zarządzania jakością: „Zgłoszenie problemu/zadania dla Działu Informatyki”. § 2. Ilekroć w Zasadach jest mowa o:

1. **Helpdesk** - rozumie się przez to pracowników Działu Informatyki przyjmujących i realizujących zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania komputerowego.
2. **Sprzęcie komputerowym** - rozumie się przez to komputer oraz urządzenia peryferyjne, w tym. monitor, drukarka, skaner, wymagające do swojego działania połączenia z komputerem.

§ 3.

1. Zgłaszanie problemów z użytkowaniem sprzętu komputerowego i udzielanie pomocy użytkownikowi odbywa się w następujący sposób:
   a. Użytkownik zgłasza awarię do, Helpdesk, który prowadzi rejestr zgłoszeń problemów.
   b. Helpdesk rozwiązuje zgłoszony problem lub przekazuje zlecenie naprawy do realizacji przez konkretnego pracownika Działu Informatyki.
2. Pracownik Helpdesk:
   a. Nawiązuje kontakt z użytkownikiem.
   b. Dokonuje oceny problemu.
   c. Podejmuje działania mające na celu usunięcie zaistniałego problemu.
   d. W przypadku braku możliwości usunięcia problemu ze sprzętem komputerowym, zgłasza do serwisu zewnętrznego w celu dokonania naprawy serwisowej.
3. Helpdesk informuje użytkownika o braku możliwości naprawy sprzętu we własnym zakresie oraz przekazuje sprzęt komputerowy do serwisu i przedstawia użytkownikowi możliwości udostępnienia sprzętu zastępczego na czas naprawy.

§ 4.

W przypadku konieczności oddania sprzętu komputerowego do zewnętrznego serwisu – pracownik Działu Informatyki, który ma przypisane dane zgłoszenie, wymontowuje i zabezpiecza dysk twardy oraz inne nośniki danych zainstalowane w danym sprzęcie. § 5.

W przypadku konieczności przekazania dysku komputera do naprawy poza miejsce użytkowania komputera:

a. Pracownik Helpdesk 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,
b. W przypadku awarii dysku twardego i konieczności podjęcia próby odtworzenia danych, zadanie to powierzane jest specjalistycznym firmom zewnętrznym, na podstawie zawartych umów.

Załącznik 4
do Instrukcji Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka
Warszawa, ……

Pieczęć Instytutu

Zakres uprawnień do systemów informatycznych IMiD

Imię i Nazwisko……..… **Stanowisko**……
Komórka organizacyjna /telefon ……..

Jednostki CliniNet ……

PESEL…… **PWZ**…….. **Numer infomedica** ……..…. (nadaje dział Kadr)
Czy użytkownik posiada upoważnienie do przetwarzania danych w IMiD [ ] Tak [ ] Nie

Zakres uprawnień CliniNet [ ] Lekarz [ ] Podstawowe[1]

Dodatkowe uprawnienia [ ] Diagnostyka [ ] STER [ ] Apteczka oddziałowa [ ] Gaxam
[ ] EOD [ ] E-Zamównienia (OPK)…….

Infomedica

Kadry		WP		Kasa		Rej. Vat	
Płace		ZP		Koszty		SWD	
Grafiki		FK		Rej. Bankowy		Windykacja	
Wykazy		Budżetowanie		Rej. Sprzedaży		GM	
ST		Imp/Expo		Rej. Zakupów			

Poczta elektroniczna [ ] Nie [ ] Tak

Dodatkowe Aliasy[2] [ ] Nie [ ] Tak-……..

Dostęp do domeny [ ] Nie [ ] Tak -domena instytut.imid.med.pl

Dostęp do zasobów sieciowych[3] [ ] Nie [ ] Tak …….

……

Pieczęć i podpis bezpośredniego przełożonego

Przyjęłam\Przyjąłem do wiadomości

…….
Data i podpis użytkownika

……..
Akceptacja Administratora Systemu Informatycznego

[1] Uprawnienia Pielęgniarka/Położna/Pomoc medyczna

[2] Dodatkowe adresy – główne kliniki\poradnie\kierownicy

[3] Dostęp do wspólnych udostępnionych folderów np. genetyka, dzial_it, por_metaboliczna

Jednostki CliniNet – proszę wpisać do jakich jednostek ma być dostęp w CliniNecie

*- w przypadku potrzeby dodatkowego aliasu (domyślnie jest to imie.nazwisko@imid.med.pl)

Załącznik nr 5 Do Instrukcji Zarządzania Systemami Informatycznymi w Instytucie Matki i Dziecka

Rejestr kopii zapasowych

Lp.	Imię nazwisko osoby wykonującej kopię	Opis kopii zapasowej	Nazwa systemu lub konta użytkownika	Numer ewidencyjny pod którym zarejestrowano kopię	Rodzaj kopii (Dzienna/ Tygodniowa/ Miesięczna)	Miejsce przechowywania kopii	Data Podpis	Uwagi