– WYCIĄG –

Z REGULAMINU

OCHRONY DANYCH OSOBOWYCH

w CENTRUM MEDYCZNYM KSZTAŁCENIA

PODYPLOMOWEGO

CENTRUM MEDYCZNE KSZTAŁCENIA PODYPLOMOWEGO | CENTRE OF POSTGRADUATE MEDICAL EDUCATION

DEFINICJE

Ilekroć w niniejszym regulaminie jest mowa o:

1) Administratorze – rozumie się przez to Administratora danych, którym jest *Centrum Medyczne Kształcenia Podyplomowego z siedzibą w Warszawie przy ulicy Marymonckiej 99/103, 01-813 Warszawa;*
2) Administratorze systemów informatycznych (lub „ASI") – rozumie się przez to osobę fizyczną wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane Ustawą i Rozporządzeniem. W przypadku niewyznaczenia ASI, jego obowiązki wykonuje Administrator osobiście lub za pośrednictwem pracowników lub współpracowników wewnętrznej służby informatycznej lub podmiotu zewnętrznego, działającego na zlecenie Administratora.
3) Danych osobowych (lub „dane") – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;
5) Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;
6) Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
7) Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE

§ 1.

W celu zapewnienia ochrony przetwarzanych danych osobowych, zarówno za pomocą systemów informatycznych jak i w wersji papierowej, Administrator wdrożył politykę bezpieczeństwa przetwarzania danych osobowych oraz instrukcję zarządzania systemem informatycznym, które stanowią odpowiednio Załącznik nr 1 i Załącznik nr 2 do Zarządzenia Dyrektora CMKP w sprawie wprowadzenia w Centrum Medycznym Kształcenia Podyplomowego: „Polityki Bezpieczeństwa w CMKP", „Instrukcji Zarządzania Systemem Informatycznym w CMKP", „Regulaminu Ochrony Danych Osobowych w CMKP". Celem jak najlepszego zapoznania pracowników i współpracowników z zasadami ochrony danych osobowych wdraża się również niniejszy regulamin, na który składają się postanowienia zawarte w polityce bezpieczeństwa oraz instrukcji zarządzania, przydatne dla każdej osoby przetwarzającej dane podczas codziennego wykonywania obowiązków zawodowych.

§ 5.

1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do Inspektora Ochrony Danych z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez Inspektora Ochrony Danych odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych, których wątpliwość dotyczy, należy, do czasu rozstrzygnięcia

wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 7.

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych, jak również wszelkie informacje, które powziął w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej.

§ 8.

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są, w miarę możliwości, w szafach lub pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba, która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tę okoliczność Inspektorowi Ochrony Danych oraz Administratorowi.
4. Inspektor Ochrony Danych lub Administrator w zakresie swoich kompetencji podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

§ 9.

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.

5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności Osoby upoważnionej.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

§ 10.

1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić Inspektora Ochrony Danych lub Administratora.

POLITYKA HASEŁ

§ 12.

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora systemu informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemów informatycznych Administratora jest obowiązany do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ich ujawnienia;
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora systemu informatycznego;
   4) poinformowania administratora systemu informatycznego oraz Inspektora ochrony danych o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
   6) stosowania haseł nieposiadających w swojej strukturze części loginu;
   7) stosowania haseł niebędących zbliżonymi do poprzednich (np. Tadeusz$2013 - Tadeusz$2014);
   8) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.
5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
6. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   4) udostępnianie haseł innym użytkownikom;

5) przeprowadzanie prób łamania haseł;

6) wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI

§ 13.

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych Administratora powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnienie należy bezzwłocznie powiadomić Administratora systemu informatycznego oraz Inspektora Ochrony Danych.
5. Dane osobowe wrażliwe lub informacje poufne Administratora, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi systemu informatycznego oraz Inspektorowi Ochrony Danych.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

§ 14.

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym, tj. brak wykonywania jakichkolwiek czynności przez okres 15 minut w systemie informatycznym, powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem przed odejściem od stanowiska.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć ich utraty.
5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:

1) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;

2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§ 15.

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki poczty elektronicznej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna prowadzona przez pracownika, a niezwiązana z działalnością Administratora, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej.
6. Użytkownicy dokonujący wysyłki korespondencji masowej poza CMKP, obowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW). sytuacji stanowiących naruszenie przyjętych zasad bezpieczeństwa
7. Zabronione jest:
   1) wysyłanie materiałów służbowych zawierających dane osobowe lub dane poufne na konta prywatne (np. celem pracy nad dokumentami w domu);
   2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;
   3) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   4) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe;
   5) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
   6) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
   7) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem – w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu informatycznego;
   8) posługiwanie się służbowym adresem skrzynki pocztowej w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;

9) wykorzystywanie służbowej poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§ 16.

1. Dostęp użytkowników do sieci publicznej (Internet) jest ograniczony do niezbędnego minimum na danym stanowisku pracy.
2. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§ 17.

1. Każdy użytkownik wymiennych nośników elektronicznych, użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do zasad określonych w ust. 2.
2. Podczas korzystania z nośników elektronicznych, zdalnych dostępów do sieci służbowej VPN oraz elektronicznych kart dostępu poza obszarem przetwarzania danych:
   1) zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
   2) komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować;
   3) użytkownik wykonując czynności zawodowe lub umowne w domu dba o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
   4) zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
   5) zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora;
   6) w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub Administratora systemu informatycznego. Bezpośredni przełożony lub Administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Inspektora Ochrony Danych, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez administratora danych;
   7) problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi systemu informatycznego.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§ 18.

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,

3) tablety,
4) smartphony,
5) drukarki,
6) modemy,
7) monitory,
8) routery,
9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.

2. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, Administrator systemu informatycznego informuje o powyższym Inspektora Ochrony Danych.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik przed dokonaniem zmiany konfiguracji przekazanego sprzętu komputerowego oraz przed instalacją lub usunięciem oprogramowania (w tym też prywatnego oprogramowania) musi powiadomić dział IT o chęci dokonania takiego działania.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ

§ 19.

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji zawierających dane osobowe lub informacji poufnych u Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych”) haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne u Administratora jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających dane osobowe lub informacje poufne.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

§ 20.

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

4. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik skontaktuje się z Administratorem systemu informatycznego.

POSTANOWIENIA KOŃCOWE

§ 21.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, w efekcie którego nastąpiło udostępnienie informacji zawierających dane osobowe lub informacji poufnych osobie nieupoważnionej, potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

– WYCIĄG –

Z POLITYKI BEZPIECZEŃSTWA

w CENTRUM MEDYCZNYM KSZTAŁCENIA

PODYPLOMOWEGO

CENTRUM MEDYCZNE KSZTAŁCENIA PODYPLOMOWEGO | CENTRE OF POSTGRADUATE MEDICAL EDUCATION

WSTĘP

Celem wdrożenia niniejszej dokumentacji jest ochrona interesów osób, których dane dotyczą poprzez zapewnienie należytej, adekwatnej do przewidywanych zagrożeń oraz kategorii przetwarzanych danych, ochrony posiadanych zasobów informacyjnych.

Poprzez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.

Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie zbiory danych osobowych przetwarzane przez administratora danych, zarówno w formie elektronicznej, jak i papierowej oraz dane osobowe przetwarzane poza zbiorami danych.

Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby, przy pomocy których Administrator danych wykonuje swoje czynności, mające dostęp do danych osobowych.

Dodatkowo, tworzy się Regulamin ochrony danych jako wyciąg najważniejszych zasad i procedur bezpieczeństwa obowiązujący wszystkie osoby przetwarzające dane osobowe.

DEFINICJE

§1

Użyte w niniejszej dokumentacji przetwarzania danych osobowych definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą dokumentacją oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych. Ilekroć w niniejszej polityce bezpieczeństwa jest mowa o:

1) Administratorze – rozumie się przez to Administratora danych, którym jest *Centrum Medyczne Kształcenia Podyplomowego z siedzibą w Warszawie przy ulicy Marymonckiej 99/103, 01-813 Warszawa*;
2) Administratorze systemów informatycznych (lub „ASI") – rozumie się przez to osobę fizyczną wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane Ustawą i Rozporządzeniem. W przypadku niewyznaczenia ASI, jego obowiązki wykonuje Administrator osobiście lub za pośrednictwem pracowników lub współpracowników wewnętrznej służby informatycznej lub podmiotu zewnętrznego, działającego na zlecenie Administratora.
3) Danych osobowych (lub „danych") – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) Dokumentacji przetwarzania danych osobowych – rozumie się przez to politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
5) Identyfikatorze (loginie) użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
6) Osobie fizycznej możliwej do zidentyfikowania – jest to osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

7) Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora upoważnienie do przetwarzania danych;

8) Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;

9) Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;

10) Użytkowniku uprzywilejowanym – rozumie się przez to osobę upoważnioną, posiadającą wyższe niż standardowo przyznawane na danym stanowisku, uprawnienia w systemie informatycznym;

11) Użytkowniku systemu – rozumie się przez to osobę upoważnioną, która otrzymała dostęp do sieci LAN umożliwiający korzystanie z sieci Internet oraz login i hasło do systemu;

12) Załącznikach – należy przez to rozumieć wzory dokumentów; Administrator może przedmiotowe wzory zastąpić wydrukami z systemów komputerowych lub innymi dokumentami o treści zgodnej z przepisami powszechnie obowiązującego prawa;

13) Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE

§2

1. W celu zapewnienia ochrony przetwarzanych danych osobowych, zarówno za pomocą systemów informatycznych jak i w wersji papierowej, Administrator wdraża niniejszą politykę bezpieczeństwa.
2. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była rozliczalność, integralność i poufność danych, gdzie przez:
   1) rozliczalność – rozumie się właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   2) integralność danych – rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) poufność danych – rozumie się właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.
3. Administrator deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych.
4. Administrator nadzoruje jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane.

§4

1. Polityka bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody Administratora.

2. Dla codziennych potrzeb pracowników i współpracowników tworzy się Regulamin ochrony danych osobowych zawierający zasady przetwarzania danych osobowych obowiązujące u Administratora.
3. Regulamin jest jawny i udostępniany w sposób powszechnie przyjęty u Administratora wszystkim pracownikom i współpracownikom.

PRZETWARZANIE DANYCH

§11

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
   1) osoba, której dane dotyczą wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
   2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
   3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
   4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
   5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. W przypadku przetwarzania danych osobowych wrażliwych (informacje ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym),
3. Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektronicznej należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219) oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, z późn. zm.), które przewidują dalej idącą ochronę.

§12

1. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
2. Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
3. Zgoda na przetwarzanie danych osobowych może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator obowiązany jest usunąć wszystkie dane osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie.
4. Zaleca się odbieranie zgody w postaci możliwej do późniejszego udowodnienia (np. pisemnie, w ramach systemu informatycznego po zastosowaniu metody dwustopniowego uwiarygodniania, jako nagranie przeprowadzonej rozmowy telefonicznej – po poinformowaniu rozmówcy o prowadzonej rejestracji).

§13

1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do Inspektora Ochrony Danych z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez Inspektora Ochrony Danych odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotyczy należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§27

1. Każdy, kto przetwarza dane osobowe, obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp, sposoby zabezpieczania danych jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych trzeba zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.
4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument trzeba zaszyfrować, a hasło przesłać , w miarę możliwości innym środkiem komunikacji elektronicznej.

§28

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy nie może przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba, która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność Inspektorowi Ochrony Danych oraz Administratorowi.
4. Inspektor Ochrony Danych oraz Administrator, w zakresie swoich kompetencji, podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

§29

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko, zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia (zaleca się, aby niszczarka spełniała wymogi normy DIN 66399, klasa bezpieczeństwa nie niższa niż 3) lub za pośrednictwem firmy zajmującej

się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.

3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności Osoby upoważnionej.
6. Szczegółowy opis środków bezpieczeństwa zastosowanych przez Administratora wskazany został w Załączniku nr 2 „Wykazy - obszary, zbiory i przepływy" do polityki bezpieczeństwa.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

§30

1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych osoba, która jako pierwsza stwierdziła możliwość naruszenia zasad bezpieczeństwa, niezwłocznie zawiadamia Inspektora Ochrony Danych lub Administratora o dostrzeżonych lub podejrzewanych naruszeniach.

POSTANOWIENIA KOŃCOWE

§31

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.
2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany Dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.
3. Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Dokumentacji przetwarzania danych osobowych.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, w efekcie którego nastąpiło udostępnienie informacji zawierających dane osobowe lub informacji poufnych osobie nieupoważnionej, potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

– WYCIĄG –

Z INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM w CENTRUM MEDYCZNYM KSZTAŁCENIA PODYPLOMOWEGO

CENTRUM MEDYCZNE KSZTAŁCENIA PODYPLOMOWEGO | CENTRE OF POSTGRADUATE MEDICAL EDUCATION

Tabela nr 1

Lp.	OPIS WYMAGANYCH ROZWIĄZAŃ TECHNICZNYCH LUB ORGANIZACYJNYCH
I.	1. Obszar, w którym przetwarzane są dane osobowe zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. 2. Przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
II.	
III.	
IV.	
V.	Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
VI.	
VII.	
VIII.	W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
IX.	Urządzenia i nośniki zawierające dane osobowe wrażliwe (sensytywne), przekazywane poza obszar, w którym przetwarzane są dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.
X.	
XII.	
XIII.	

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

ZASADY OGÓLNE

§2

1. Przydzielanie uprawnień do systemu informatycznego realizowane jest w oparciu o następujące zasady:
   1) „minimalnych przywilejów" – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;
   2) „wiedzy koniecznej" – użytkownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań;
   3) „domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.
2. Dostęp do systemu informatycznego mogą posiadać, w zależności od wykonywanych czynności służbowych lub umownych:
   1) osoby, przy pomocy których Administrator wykonuje swoje czynności, w szczególności:
      a) osoby zatrudnione na podstawie umów cywilnoprawnych;
      b) pracownicy lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz Administratora;
3. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień (przywilejów) będzie kwalifikowane jako incydent związany z bezpieczeństwem informacji.
4. Użytkownikowi systemu informatycznego zostaje nadany dostęp po:
   1) zapoznaniu z przepisami, w tym niniejszą dokumentacją przetwarzania danych osobowych, dotyczącymi ochrony danych osobowych;
   2) podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych, oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych;
   3) otrzymaniu upoważnienia do przetwarzania danych osobowych.

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

§8

Niniejszy rozdział reguluje tryb przydzielania haseł, wymogi dotyczące stopnia ich złożoności oraz wskazuje osoby odpowiedzialne za przydział haseł. Zawarte w niniejszym rozdziale procedury odnoszą się również do:

1) możliwych zagrożeń i konsekwencji związanych z tzw. utratą tożsamości elektronicznej (tj. utratą danych służących uwierzytelnieniu, co może skutkować pozyskaniem tych danych przez osoby nieuprawnione);
2) zalecanych sposobów korzystania z przeglądarek internetowych.

ZASADY OGÓLNE

§9

1. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora systemu informatycznego) i jego przechowywanie.

POLITYKA HASEŁ

§10

Każdy użytkownik posiadający dostęp do systemów informatycznych Administratora jest obowiązany do:

1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora systemu informatycznego;
4) poinformowania administratora systemu informatycznego oraz Inspektora Ochrony Danych o podejrzeniu lub rzeczywistym ujawnieniu hasła;
5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
6) stosowania haseł nieposiadających w swojej strukturze części login;
7) Stosowania haseł niebędących zbliżonymi do poprzednich (np. Tadeusz$2013 - Tadeusz$2014);
8) Zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.

§11

1. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
2. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   4) udostępnianie haseł innym użytkownikom;
   5) przeprowadzanie prób łamania haseł;
   6) wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI

§13

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji wewnętrznych Administratora powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.

2. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada administrator systemu informatycznego.
3. Przekazywanie kluczy użytkownikom odbywa się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
4. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
5. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia, należy bezzwłocznie powiadomić Administratora systemu informatycznego oraz Inspektora Ochrony Danych.
6. Dane osobowe wrażliwe lub informacje wewnętrzne Administratora, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
7. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
8. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi systemu informatycznego oraz Inspektora Ochrony Danych.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

§14

Niniejszy rozdział opisuje kolejne czynności, jakie należy wykonać w celu uruchomienia systemu informatycznego, a w szczególności zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Przestrzeganie określonych w Instrukcji zasad ma na celu zachowanie poufności haseł oraz uniemożliwienie nieuprawnionego przetwarzania danych. Zawarte w niniejszym rozdziale procedury obejmują również:

1) metody postępowania w sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy;
2) metody postępowania w sytuacji, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba;
3) sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu, np. w razie braku możliwości zalogowania się użytkownika na jego konto czy też w sytuacji stwierdzenia fizycznej ingerencji w przetwarzane dane bądź użytkowane narzędzia programowe lub sprzętowe.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY

§15

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym, tj. brak wykonywania jakichkolwiek czynności przez okres 15 minut w systemie informatycznym, powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem przed odejściem od stanowiska.
3. Przed zakończeniem pracy użytkownik ma obowiązek upewnić się, czy dane zostały zapisane, aby uniknąć utraty danych.

4. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
5. W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba, trzeba tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:
    1) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
    2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§16

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki poczty elektronicznej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna niezwiązana z działalnością Administratora powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej.
6. Użytkownicy dokonujący wysyłki korespondencji masowej poza CMKP, obowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW).
7. Zabronione jest:
    1) wysyłanie materiałów służbowych zawierających dane osobowe lub dane poufne na konta prywatne (np. celem pracy nad dokumentami w domu);
    2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;
    3) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
    4) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe;
    5) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
    6) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;

7) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu informatycznego;

8) posługiwanie się służbowym adresem skrzynki pocztowej w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;

9) wykorzystywanie służbowej poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§17

1. Dostęp użytkowników do sieci publicznej (Internet) jest ograniczony do niezbędnego minimum na danym stanowisku pracy.
2. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.
3. Dostęp do protokołu wymiany plików możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.
4. Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez Inspektora Ochrony Danych

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§18

1. Każdy użytkownik wymiennych nośników elektronicznych, użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do zasad określonych w ust. 2.
2. Podczas korzystania z nośników elektronicznych, zdalnych dostępów do sieci służbowej VPN oraz elektronicznych kart dostępu poza obszarem przetwarzania danych:
   1) zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
   2) komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować;
   3) użytkownik wykonując czynności zawodowe lub umowne w domu, powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
   4) zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
   5) zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora;
   6) w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego, Inspektora Ochrony Danych lub Administratora systemu informatycznego. Bezpośredni przełożony lub Administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Inspektora Ochrony Danych, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;

7) problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi systemu informatycznego.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§23

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne;
   2) komputery przenośne;
   3) tablety;
   4) smartphony;
   5) drukarki;
   6) modemy;
   7) monitory;
   8) routery;
   9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Przekazanie sprzętu jest to czynność polegająca na dostarczeniu sprzętu komputowego wraz z odpowiednim oprogramowaniem użytkownikowi.
3. Administrator systemu informatycznego odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik przed dokonaniem zmiany konfiguracji przekazanego sprzętu komputerowego oraz przed instalacją lub usunięciem oprogramowania (w tym też prywatnego oprogramowania) musi powiadomić dział IT o chęci dokonania takiego działania.
6. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ

§24

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji zawierających dane osobowe lub informacji poufnych u Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne u Administratora jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających dane osobowe lub informacje poufne.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

§27

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
4. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik ma obowiązek skontaktować się z Administratorem systemu informatycznego.

§30

1. Wszelkie naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora przeprowadzane są – o ile to możliwe – przez upoważnionych pracowników Administratora.

POSTANOWIENIA KOŃCOWE

§31

5. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.
6. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany Dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.
7. Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Dokumentacji przetwarzania danych osobowych
8. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, w efekcie którego nastąpiło udostępnienie informacji zawierających dane osobowe lub informacji poufnych osobie nieupoważnionej, potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.