

Załącznik do Zarządzenia Rektora nr 154/2021 z dnia 31.12.2021 r.

Instrukcja zarządzania systemem informatycznym w Uniwersytecie Medycznym w Białymstoku

Rozdział 1.....	3
Postanowienia ogólne	3
Rozdział 2.....	3
Procedura nadawania uprawnień do systemu informatycznego, w którym przetwarzane są dane osobowe	3
Zarządzanie uprawnieniami administratorów	4
Rozdział 3.....	4
Metody i środki uwierzytelnienia	4
Indywidualne konta i hasła użytkowników:	4
Konta administratora:	5
Hasła administratora	6
Rozdział 4.....	6
Procedura rozpoczęcia, zawieszenia i zakończenia pracy.....	6
Zawieszenie pracy	7
Zakończenie pracy	7
Rozdział 5.....	7
Procedura tworzenia kopii zapasowych.....	7
Rozdział 6.....	8
Procedura użytkowania komputerów przenośnych i innych elektronicznych nośników informacji np. smartfon, tablet, pendrive	8
Rozdział 7.....	9
Procedura niszczenia/czyszczenia nośników danych.....	9
Rozdział 8.....	10
Procedura wykonywania przeglądów i konserwacji	10
Aktualizacje oprogramowania.....	11
Rozdział 9.....	11
Procedura zabezpieczenia systemu informatycznego	11
Rozdział 10.....	13
Zabezpieczenia fizyczne i techniczne	13
Rozdział 11.....	14
Plan ciągłości działania	14
Plan awaryjny odtworzenia systemu informatycznego po awarii krytycznej.....	14
Plan awaryjny na wypadek przerwy w zasilaniu sieci komputerowej	15
Rozdział 12.....	15
Postanowienia końcowe	15

Rozdział 1

Postanowienia ogólne

Niniejsza „Instrukcja zarządzania systemem informatycznym w Uniwersytecie Medycznym w Białymstoku” zwana dalej „Instrukcją” stanowi zestaw procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z art. 32 RODO, zabezpieczyć przetwarzane dane osobowe. Regulacje dotyczące zasad bezpieczeństwa znajdują się stronie <https://www.umb.edu.pl/bsi> zwanej dalej „BSI”.

Rozdział 2

Procedura nadawania uprawnień do systemu informatycznego, w którym przetwarzane są dane osobowe

Procedura opisuje zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym. Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieuprawnione.

1. Przyznanie, zmiana lub usunięcie uprawnień użytkownika do systemów informatycznych, w których przetwarzane są dane osobowe odbywa się na podstawie zgłoszenia przełożonego do właściwego administratora systemu.
2. Każde nadane uprawnienie do systemu informatycznego, w którym użytkownik przetwarza dane osobowe, poprzedzone jest nadaniem upoważnienia do przetwarzania danych osobowych zgodnie z procedurą nadawania upoważnień do przetwarzania danych osobowych, stanowiącą załącznik do Polityki ochrony danych osobowych.
3. Dostęp do systemu informatycznego nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu).
4. Każdy użytkownik przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym powinien:
 - a) posiadać upoważnienie do przetwarzania danych osobowych,
 - b) zapoznać się z niniejszą instrukcją,
 - c) być przeszkolonym z zasad ochrony danych osobowych w UMB przez Inspektora Ochrony Danych.
 - d) Podpisać oświadczenie o zachowaniu poufności.
5. Identyfikator użytkownika po zablokowaniu w systemie informatycznym nie może być przydzielony innej osobie.

6. Obowiązuje zasada minimalizacji uprawnień.
7. Użytkowników obowiązuje zasada pracy na własnym koncie.
8. Zabronione jest udostępnianie loginu i hasła innym osobom.

Zarządzanie uprawnieniami administratorów

1. Administratorów systemów informatycznych powołuje pisemnie Rektor.
2. Każdy Administrator systemu zobowiązany jest do bieżącej pracy na własnym profilu roboczym. Użycie głównego konta administracyjnego dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
3. Hasła do głównego konta administracyjnego znane są tylko administratorowi odpowiedzialnemu za dany system.
4. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane osobie zastępującej administratora na podstawie wniosku przełożonego (polecenia służbowego w formie ustnej lub pisemnej). Osoba ta na czas zastępstwa powinna dostać upoważnienie do przetwarzania danych osobowych w zakresie tym samym, co nieobecny administrator. Osoba zastępująca wykorzystuje własny profil logowania z uprawnieniami administratora.
5. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany uprawnień osoby zastępującej i zmiany hasła własnego (jeżeli mogła zaistnieć sytuacja poznania go przez kogoś innego).

Rozdział 3

Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, iż do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

Systemy administrowane w Uniwersytecie Medycznym w Białymstoku powinny stosować się do zasad ustalanych niniejszą Instrukcją, jak również powiązanymi z nią zarządzeniami, aplikacjami i dokumentami wspomagającymi zasadę wspomagania szeroko pojętego bezpieczeństwa zasobów informatycznych i osób w jakikolwiek sposób uczestniczących w procesach składowych ich funkcjonowania.

Indywidualne konta i hasła użytkowników:

1. Użytkownicy systemów informatycznych logują się za pomocą konta zintegrowanego z usługą Active Directory.

2. Konto w usłudze Active Directory zakładane jest automatycznie po wprowadzeniu do programu kadrowego informacji o zatrudnieniu pracownika.
3. Pierwsze domyślne hasło generowane jest zgodnie z zasadą opisaną na stronie <https://www.umb.edu.pl/bsi>.
4. Po otrzymaniu loginu i hasła oraz po zalogowaniu się do komputera, użytkownik zobowiązany jest do bezzwłocznej zmiany hasła.
Hasło można dodatkowo zmienić za pomocą strony <https://haslo.umb.edu.pl>.
5. Hasło traci swoją ważność po czasie opisanym w BSI. W przypadku zablokowania konta, hasło jest ustawiane na domyślne przez pracowników Działu Informatyki, lub samodzielnie przez użytkownika za pomocą strony <https://haslo.umb.edu.pl>.
6. Hasło powinno spełniać minimalne wymagania bezpieczeństwa opisane w BSI.
7. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy, jako haseł wykorzystywać: imion, nazwisk, inicjałów, dat, itp.
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
9. Zabronione jest przekazywanie haseł do kont innym użytkownikom.

Konta administratora:

1. Każdy administrator systemów informatycznych loguje się za pomocą indywidualnego konta, dla którego nadane są uprawnienia administratora.
2. Obowiązuje zasada nie używania głównych kont administracyjnych, a czynności administracyjne, o ile to możliwe, powinny być wykonywane za pomocą kont personalnych z nadanymi uprawnieniami administracyjnymi.
3. Domyślne hasło generowane jest zgodnie z zasadą opisaną w BSI. Administrator systemu po zalogowaniu zobowiązany jest do niezwłocznej zmiany tego hasła za pomocą strony <https://haslo.umb.edu.pl>.
4. Hasło powinno spełniać minimalne wymagania bezpieczeństwa opisanego w BSI.
5. Zaleca się zmianę hasła w przypadku uzasadnionego podejrzenia wpływającego na możliwy nieuprawniony dostęp do zasobów nim chronionych. Zaleca się zmianę haseł nie rzadziej, niż co okres opisany w BSI. W przypadku, jeżeli system informatyczny nie wymusza zmiany haseł to czynność zmiany hasła spoczywa na użytkowniku systemu.
6. Administrator zobowiązuje się do zachowania hasła w poufności, nawet po utracie jego ważności.
7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

Hasła administratora

1. Sposób budowy hasła administratora opisany jest w BSI.
2. Administrator systemu zobowiązany jest zmieniać swoje hasło zgodnie z procedurą zmiany hasła dla administratorów opisaną w BSI.
3. Administrator zobowiązany jest do utworzenia głównego hasła administracyjnego w systemie i umieszczeniu go w zamkniętej kopercie, w sejfie.
4. W przypadku jego awaryjnego wykorzystania ma zastosowanie wewnętrzna instrukcja Bezpieczeństwa Systemów Informatycznych. Fakt ten powinien być odnotowany odrębną notatką służbową oraz informacja o zdarzeniu powinna być przekazana Inspektorowi Danych Osobowych UMB.
5. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Kanclerza osobie zastępującej administratora. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.
6. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie usunąć jej uprawnienia i zmienić hasła, do których osoba miała dostęp.

Rozdział 4

Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

Rozpoczęcie pracy w systemie bądź w aplikacji:

- 1) Użytkownik po uruchomieniu komputera wchodzącego w skład systemu informatycznego, podłączonego fizycznie do sieci lokalnej loguje się podając własny identyfikator (login) i hasło dostępu.
- 2) Użytkownik jest zobowiązany do powiadomienia Działu Informatyki o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje. Po nieudanych próbach logowania konto może zostać zablokowane.
- 3) W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest skontaktować się z pracownikiem Działu Informatyki w celu otrzymania instrukcji dalszego postępowania.

Zawieszenie pracy

1. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. pracownikom innych działów, interesantom) wglądu do danych wyświetlanych na monitorach komputerowych tzw. polityka czystego ekranu.
2. Przy każdorazowym opuszczeniu stanowiska pracy, należy dopilnować, aby na ekranie nie były wyświetlane dane osobowe.
3. Przy opuszczeniu stanowiska pracy na dłużej np. opuszczeniu pokoju przez użytkownika, jest on zobowiązany zabezpieczyć dostęp do komputera np. zablokować hasłem lub wylogować się z systemu. Jeżeli tego nie uczyni, system winien automatycznie aktywować wygaszanie ekranu po upływie czasu regulowanego w zasadach przedstawionych w BSI.

Zakończenie pracy

Po zakończeniu pracy, użytkownik zobowiązany jest:

- 1) zamknąć system lub aplikację (wylogować się),
- 2) wyłączyć sprzęt komputerowy,
- 3) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz wszystkie nośniki, na których znajdują się dane osobowe.

Rozdział 5

Procedura tworzenia kopii zapasowych

Celem procedury jest zabezpieczenie danych osobowych przetwarzanych w systemie informatycznym poprzez tworzenie kopii zapasowych.

- 1) Za proces tworzenia kopii zapasowych systemu informatycznego odpowiada administrator lub osoba specjalnie do tego celu wyznaczona.
- 2) W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu informatycznego zobowiązani są do przechowywania danych tak, aby możliwe było zabezpieczenie ich poprzez wykonanie kopii zapasowych. Użytkownicy systemu są zobowiązani do lokalnego sporządzania kopii zapasowych przetwarzanych danych osobowych na nośniku wymiennym w przypadku braku możliwości wykonania ich kopii z poziomu centralnego.
- 3) Kopie zapasowe systemów informatycznych i baz danych przetwarzających dane osobowe tworzone są codziennie przy wykorzystywaniu specjalnie przeznaczonych do tego celu urządzeń i oprogramowania.

- 4) Do tworzenia kopii zapasowych wykorzystywane urządzenia i oprogramowanie wchodzące w skład systemu informatycznego na nośnikach adekwatnych do rodzaju urządzenia.
- 5) W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy, muszą być okresowo (co najmniej raz na pół roku), sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego.
- 6) Testy przydatności kopii zapasowych oraz ich rezultaty są odnotowywane przez administratora systemu informatycznego w dzienniku zdarzeń serwisowych.
- 7) Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przypadku, gdy jest to niemożliwe nośniki te podlegają fizycznemu zniszczeniu w sposób adekwatny do typu nośnika, uniemożliwiający odczytanie zapisanych na nich danych.

Rozdział 6

Procedura użytkowania komputerów przenośnych i innych elektronicznych nośników informacji np. smartfon, tablet, pendrive

Procedura określa sposób postępowania z nośnikami danych, na których znajdują się dane osobowe, celem zabezpieczenia ich przed utratą, zniszczeniem, kradzieżą, dostępem osób nieupoważnionych.

1. Komputery przenośne i inne elektroniczne nośniki informacji są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Użytkownicy komputerów przenośnych i innych urządzeń przenośnych np. tablet, smartfon, pendrive, na których są przetwarzane dane osobowe, wynoszonych poza Uczelnię zobowiązani są do przestrzegania poniższych zasad bezpieczeństwa:
 - a) dane osobowe wynoszone poza Uczelnię na komputerach przenośnych i innych urządzeniach przenośnych powinny być szyfrowane przy użyciu metod BSI,
 - b) w przypadku kradzieży lub zgubienia komputera przenośnego lub urządzenia, Użytkownik powinien natychmiast powiadomić o tym Inspektora Ochrony Danych - osobę odpowiedzialną za ochronę danych (IOD), kierownika Działu Informatyki i bezpośredniego przełożonego, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane,

- c) Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego i urządzeń przenośnych w czasie transportu i niepozostawianie ich w samochodzie bez nadzoru,
 - d) pracując na komputerze / urządzeniu przenośnym w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na ekranie informacje przed wglądem osób nieupoważnionych,
 - e) w przypadku pozostawiania komputerów / urządzeń przenośnych, nośników danych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach,
 - f) Użytkownik komputera/urządzenia przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa,
 - g) na komputerach/urządzeniach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, (jeśli to możliwe) znajdować się dane osobowe,
 - h) Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania (kasowania) danych osobowych z komputerów przenośnych i innych elektronicznych nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
3. W sytuacji przekazywania/przesyłania nośników z danymi osobowymi np. pendrive, płyta cd/dvd poza teren Uczelni należy stosować następujące zasady bezpieczeństwa:
- a) adresat powinien zostać powiadomiony o przesyłce,
 - b) nadawca powinien sporządzić kopię przesyłanych danych,
 - c) dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
 - d) należy zastosować bezpieczne koperty depozytowe, a przesyłka pakowana dwukrotnie w celu utrudnienia dostępu do nich,
 - e) przesyłka powinna być przesłana przez kuriera,
 - f) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
4. Procedura dopuszczalności nośnika jest regulowana za pomocą instrukcji zawartych przez BSI.
5. W zakresie nieuregulowanym w niniejszej procedurze zasady używania komputerów przenośnych reguluje w Uczelni odrębne zarządzenie Rektora.

Rozdział 7

Procedura niszczenia/czyszczenia nośników danych

1. Nośniki danych takie jak: pendrive, płyty CD/DVD/ smartfony, które są przeznaczone do likwidacji np. uszkodzone, przestarzałe powinny być niszczone w sposób fizyczny przez pracowników Działu

Informatycznego i Teletransmisji lub w firmie specjalistycznej. Niszczenie powinno być potwierdzone protokołem.

2. Nośniki danych takie jak twarde dyski powinny być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza Uczelnię np. sprzedaż, darowizna.

Rozdział 8

Procedura wykonywania przeglądów i konserwacji

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

Przeglądy i konserwacje systemu informatycznego i aplikacji:

- 1) Administrator Systemu Informatycznego odpowiada za bezawaryjną pracę systemu informatycznego, w tym: aplikacji serwerowych, baz danych, poczty email.
- 2) Administrator Systemu Informatycznego odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
- 3) Administrator Systemu Informatycznego odpowiada za sprawdzanie poprawności działania systemu informatycznego, w tym: serwerów, baz danych, poczty email.
- 4) Administrator Systemu Informatycznego odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
- 5) Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w odrębnej umowie lub na podstawie upoważnienia uwzględnieniem klauzuli dotyczącej ochrony danych.
- 6) Czynności konserwacyjne i naprawcze wykonywane doraźnie w Uczelni przez osoby z zewnętrznych serwisów, muszą być wykonywane pod nadzorem pracowników Działu Informatyki. Osoby wykonujące czynności konserwacyjne i naprawcze zobowiązane są do zachowania w poufności informacji, w tym danych osobowych, potwierdzając to pisemnym oświadczeniem.
- 7) Rekomendowane jest korzystanie z serwisu, który dokonuje napraw na miejscu w Uczelni.
- 8) W przypadku napraw dokonywanych na zewnątrz z komputerów należy dołożyć starań, żeby urządzenia przekazywane były bez danych osobowych. W tym celu należy np. wymontować dysk i wszelkie nośniki, z urządzeń mobilnych karty pamięci lub zaszyfrować dane.

Aktualizacje oprogramowania

1. Administrator Systemu Informatycznego odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
2. Administrator Systemu Informatycznego odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.
3. Praca administratora w zakresie czynności opisanych w instrukcji jest dokumentowana na serwerze w postaci rejestru zdarzeń.

Rozdział 9

Procedura zabezpieczenia systemu informatycznego

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe np. przez programy szpiegujące, hackerów

1. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej:
 - a) stosowany jest firewall,
 - b) zastosowano mechanizmy kontroli dostępu w postaci wykrywania i blokowania ataków do sieci komputerowej,
 - c) zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników.
 - d) zastosowano system antywirusowy na stacjach roboczych:
 - aktualizacja definicji wirusów odbywa się automatycznie przez system,
 - w przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik zobowiązany jest powiadomić pracownika Działu Informatyki.
2. Zabezpieczenia infrastruktury informatycznej:
 - a) zapewniono bezpieczeństwo łącza internetowego,
 - b) zapewniono zabezpieczenie infrastruktury sprzętowej w systemy ochrony danych osobowych przed skutkami awarii pamięci dyskowej,
 - c) stosuje się blokady dostępu z urządzeń zewnętrznych,
 - d) stosuje się zabezpieczenia portów fizycznych celem uniemożliwienia zmian konfiguracji przez osoby nieupoważnione,
 - e) stosuje się dezaktywację nieużywanych gniazd sieciowych,
 - f) stosuje się kontrolę dostępu do urządzeń drukujących,

- g) zabronione jest samowolne instalowanie przez użytkowników jakiegokolwiek oprogramowania, dodatkowych urządzeń np. pamięci, twardych dysków.

3. Zabezpieczenia aplikacji:

- a) w miarę możliwości technologicznych zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach /bazach danych/, serwerach plików,
- b) w ramach rozliczalności logowane są operacje tworzenia, zmiany (historii zmian), usuwania rekordu, wglądu w dane, eksportu danych do plików,
- c) kluczowe aplikacje/bazy z danymi osobowym zabezpieczono przed eksportem danych do plików (np. tekstowych, .csv, .xls),
- d) zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany,
- e) zabezpieczono testowe wersje aplikacji poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany,
- f) szyfrowanie baz danych,
- g) w kluczowych aplikacjach stosuje się terminację sesji,
- h) przechowywanie zaszyfrowanych danych w chmurze,
- i) dla aplikacji webowych stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL,
- j) formularze kontaktowe na stronach www zabezpieczono protokołem SSL,
- k) URL Aplikacji webowych są skrócone/pozbawione końcówek alfanumerycznych,
- l) jeżeli jest taka możliwość, dla aplikacji webowych zastosowano mechanizm captcha (kod z obrazka do przepisania w formularzu),
- m) Zabezpiecza się logi systemowe przed sfałszowaniem.

4. Zabezpieczenia poczty elektronicznej:

- a) stosuje się szyfrowanie poczty wychodzącej (SSL),
- b) użytkownik może korzystać z poczty elektronicznej tylko do celów służbowych,
- c) dane szczególnej kategorii powinny być wysyłane pocztą elektroniczną wyłącznie w formie zahasłowanej, hasło do odszyfrowania wysyłane/przekazywane jest inną drogą,
- d) preferowane jest również wysyłanie wiadomości w formie zahasłowanej w przypadku wysyłania danych osobowych zwykłych,
- e) użytkownik nie powinien otwierać podejrzanych wiadomości i podejrzanych załączników i przypadki podejrzanych wiadomości należy zgłaszać do Działu Informatyki,
- f) użytkownik poczty zobowiązany jest niezwłocznego i trwałego usuwania (kasowania) danych osobowych informacji po ustaniu powodu ich przechowywania.

Rozdział 10

Zabezpieczenia fizyczne i techniczne

1. Zabezpieczenia fizyczne

- a) obowiązuje kontrola dostępu do budynków i pomieszczeń (portierzy, ochrona),
- b) obowiązują zasady postępowania z kluczami do pomieszczeń uregulowane w odrębnym zarządzeniu Rektora,
- c) dostęp do pomieszczeń takich jak serwerownie mają wyłącznie upoważnione osoby,
- d) ustawienie komputerów, drukarek, ksero ogranicza dostęp osób nieupoważnionych,
- e) dane osobowe na nośnikach zabezpiecza się w szafach, biurkach zamykanych na klucz,
- f) ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze),
- g) krytyczne elementy infrastruktury zabezpieczono w zamykanych na klucz szafach serwerowych,
- h) rozdzielnie elektryczne zabezpieczono w szafach zamykanych na klucz,
- i) dostęp do serwerowni zabezpieczono drzwiami zamykanymi na klucz,
- j) dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz,
- k) obiekt/pomieszczenia chronione są przez system alarmowy / zabezpieczenia antywłamaniowe / kraty / rolety przeciwłamaniowe,
- l) kontrola dostępu do pomieszczeń serwerowni i punktów dystrybucyjnych sieci.

2. Zabezpieczenia techniczne

- a) monitoring wizyjny na terenie Uczelni,
- b) redundantna linia zasilania,
- c) zastosowano agregat prądowłórczy / UPS do serwera / UPS podtrzymujący zasilanie serwera /UPS na kluczowych elementach systemu informatycznego / sieć stabilizowaną,
- d) zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu,
- e) serwerownia wyposażona w system gaszenia gazami technicznymi / gaśnice,
- f) serwerownia z materiałów niepalnych,
- g) czujnik dymu w serwerowni,
- h) monitoring środowiskowy w serwerowni - czujnik temperaturowy,
- i) powiadomianie administratora systemu informatycznego o alertach temperatury,
- j) podłoga techniczna w serwerowni,
- k) klimatyzacja w serwerowni,
- l) archiwum - składowanie dokumentacji papierowej na podwyższeniu,

- m) monitoring środowiskowy w archiwum - czujniki wilgotności,
- n) digitalizacja dokumentów archiwalnych.

Rozdział 11

Plan ciągłości działania

Pan ciągłości działania określa czynności mające na celu podtrzymanie i usprawnienie funkcjonowania Systemu Informatycznego w Uniwersytecie Medycznym w Białymstoku. Jego zadaniem jest zapewnianie dostępu do usług i infrastruktury informatycznej a w szczególności do krytycznych procesów w godzinach wzmożonej pracy jego użytkowników.

Plan awaryjny odtworzenia systemu informatycznego po awarii krytycznej.

1. Zasady postępowania przy odtworzeniu systemu informatycznego
 - a) w przypadku stwierdzenia krytycznej awarii serwera podstawowego, osoba upoważniona - ASI (Administrator Systemów Informatycznych) zapewnia podtrzymanie dostępu do usług za pomocą serwera zapasowego, konfiguruje serwer bazowy, odtwarza dane z kopii zapasowej, postępuje zgodnie z wewnętrzną procedurą Działu Informatyki;
 - b) po przywróceniu prawidłowego funkcjonowania serwera podstawowego ASI przekierowuje do niego ruch użytkowników;
 - c) przewidywany czas operacji uruchomienia serwera zapasowego oraz przywrócenia funkcjonowania serwera podstawowego określają regulacje wewnątrz Działu Informatyki;
 - d) w przypadku nieobecności ASI, procedurę odtworzenia należy wykonać z pomocą firmy zewnętrznej, z którą Uniwersytet Medyczny w Białymstoku ma podpisaną umowę serwisową zobowiązującą tą firmę do podtrzymania funkcjonowania świadczenia danej usługi.
2. Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji alternatywnej
 - a) w przypadku braku możliwości świadczenia usług z bazowej lokalizacji serwerowni, należy zaplanowaną uprzednio lokalizację przeznaczyć na alternatywną serwerownię;
 - b) przygotowanie serwerowni wymaga: zapewnienia energii elektrycznej, UPS, łącz telekomunikacyjnych;
 - c) ASI jest odpowiedzialny za dostawę serwera zapasowego, jego konfigurację, wgranie danych z kopii zapasowych i przywrócenie świadczenia usług, zgodnie z procedurą i przewidywanym czasem wykonania tego działania regulowanymi wewnętrzną polityką bezpieczeństwa Działu Informatyki;

- d) w przypadku nieobecności ASI, procedurę odtworzenia należy wykonać z pomocą firmy zewnętrznej, na podstawie odrębnych umów, zobowiązujących firmę do dostarczenia i uruchomienia serwera zastępczego.

Plan awaryjny na wypadek przerwy w zasilaniu sieci komputerowej

W razie awarii transformatora zasilającego sieć energetyczną następuje automatycznie przełączenie na drugi transformator. Strategiczne elementy sieci komputerowej podłączone są do urządzeń UPS. W przypadku dłuższej awarii sieci zasilającej ASI zobowiązany jest do powiadomienia wszystkich użytkowników o konieczności zakończenia pracy w systemach.

W przypadku braku możliwości przywrócenia zasilania w sieci:

- 1) ASI zabezpiecza podstawowe dane,
- 2) Awaria trwająca powyżej 5 godzin wymaga uruchomienia generatora prądu.

Plan awaryjny na wypadek utraty dostępu do sieci Internet

1. W przypadku niedostępności sieci Internet awarię należy zgłaszać do operatora/dostawcy usługi.
2. W przypadku dłuższej niedostępności Internetu należy uruchomić router sieci komórkowej, jeżeli warunki techniczne i organizacyjne pozwalają na działanie w tym zakresie.

Rozdział 12

Postanowienia końcowe

W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie mają:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000).
3. Regulacje instrukcji Bezpieczeństwa Systemów Informatycznych (BSI).
4. Regulacje z zakresu zadań Administratora Systemów Informatycznych (ASI).

Pierwszy Zastępca Rektora

prof. dr hab. Marcin Moniuszko