Instrukcja zarządzania
systemem informatycznym
służącym do przetwarzania danych osobowych
w Częstochowskim Centrum Świadczeń

Wersja 1.0		**Pieczęć firmowa:**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Tomasz Salachna	2017-03-24		.

1. Wstęp....3
2. Definicje....3
3. Polityka kluczy....3
4. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej....4
5. Zabezpieczenia programów i baz przetwarzających dane osobowe....4
6. Procedura dostępu podmiotów zewnętrznych....5
7. Procedura korzystania z Internetu....6
8. Procedura korzystania z poczty elektronicznej....6
9. Procedura nadawania uprawnień do przetwarzania danych osobowych....7
9.1. Zarządzane uprawnieniami użytkowników....7
9.2. Zarządzanie uprawnieniami administratorów....8
10. Metody i środki uwierzytelnienia....8
10.1. Ogólne zasady postępowania z hasłami....8
10.2. Hasła użytkowników do sieci i serwera....8
10.3. Hasła do programów przetwarzających dane osobowe....9
10.4. Hasła administratora....9
11. Procedura rozpoczęcia, zawieszenia i zakończenia pracy....9
12. Procedura tworzenia kopii zapasowych....10
12.1. Tworzenie kopii bezpieczeństwa programu Kadrowo – płacowego....10
12.2. Tworzenie kopii bezpieczeństwa dokumentacji serwera....11
12.3. Tworzenie kopii bezpieczeństwa sklepu internetowego....11
13. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków....12
13.1. Zabezpieczenie elektronicznych nośników informacji....12
13.2. Zabezpieczenie kopii zapasowych....12
13.3. Zabezpieczenie dokumentów i wydruków....12
14. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi....13
14.1. Ochrona antywirusowa....13
14.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej....13
15. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych....14
16. Procedura wykonywania przeglądów i konserwacji....15
16.1. Przeglądy i konserwacje systemu informatycznego i aplikacji....15
16.2. Aktualizacje oprogramowania....15
16.3. Dziennik administratora....15

1. Podstawa prawna.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. Nr 992) oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z pózn. zm.)

2. Wstęp

Instrukcja stanowi zestaw procedur opisujących zasady zabezpieczania danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.

3. Definicje

1. ASI – Administrator Systemu Informatycznego. Osoba lub podmiot sprawująca zadania związane z administracją systemami, bazami lub aplikacjami ADO. Formami zatrudnienia ASI mogą być: umowa o pracę, umowa cywilno-prawna, kontrakt (umowa) z firmą informatyczną w zakresie administracji systemami informatycznymi.

4. Polityka kluczy

1. Polityka kluczy obejmuje pomieszczenia przy Al. Niepodległości 20/22, Nowowiejskiego 26 i 15
2. Obowiązuje pięciodniowy tydzień pracy, od poniedziałku do piątku, w godz. 07:30–15:30 poniedziałek, środa, czwartek, w godz. 7:30-16:00 wtorek, w godz. 7:30-15:00 piątek.
3. Upoważnienia do pobierania kluczy do pomieszczeń mają wyłącznie osoby upoważnione przez dyrektora jednostki. Upoważnienie wymaga wprowadzenia osoby do ewidencji, prowadzonej przez służbę ochrony budynku.
4. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych.
5. Klucze do pomieszczeń wydawane i zdawane są za pobraniem z pomieszczenia portierni z odnotowaniem w rejestrze papierowym.
6. Klucze do pomieszczeń szczególnie chronionych np. serwerowni wydawane są (za pobraniem / pozostają pod osobistym nadzorem osób upoważnionych)* niepotrzebne skreślić. Dostęp osób trzecich do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.
7. Klucze zapasowe przechowywane są w portierni pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą osób uprawnionych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.
8. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
9. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
10. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.

11. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń, a w szczególności wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi, ew. aktywacji alarmu.
12. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

5. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Zastosowano UPS do serwera oraz do elementów sieci typu router.
2. Użytkownicy komputerów przenośnych wynoszonych poza obszar organizacji, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa i podpisania **Załącznika 01 Regulamin użytkowania komputerów przenośnych**
3. Dane osobowe na komputerach przenośnych wynoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach.
4. W przypadku dostępu do danych osobowych przez Internet, stosuje się szyfrowanie tego połączenia (SSL lub VPN).
5. W przypadku dostępu do danych osobowych przez Internet do środków teletransmisji, wymagane jest uwierzytelnienie podanie loginu i hasła.
6. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
7. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym (np. klientom, pracownikom innych działów,) dostęp do nich.
8. Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej - komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
9. Dostęp do stacji roboczych lub systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

6. Zabezpieczenia programów i baz przetwarzających dane osobowe

1. Dostęp do danych osobowych w programie lub w bazie wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano mechanizm blokady dostępu po 5 próbach nieudanego logowania się do aplikacji.
3. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
4. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych – logi systemowe.
5. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych
6. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

7. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
8. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

7. Procedura dostępu podmiotów zewnętrznych

Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Administrator Danych.

W procedurze wyróżniono 2 rodzaje umów

- Umowa/Klauzula poufności – podpisywana z podmiotami, które mają dostęp do danych osobowych na terenie firmy / organizacji. Przykładami takich podmiotów są: zewnętrzna firma serwisująca sprzęt komputerowy, firma ochroniarska.
- Umowa powierzenia przetwarzania danych – podpisywana z podmiotami, które przetwarzają dane osobowe „na zewnątrz" w formie outsourcingu.

1. Administrator Bezpieczeństwa Informacji prowadzi rejestr podmiotów zewnętrznych, którym Administrator udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej. Patrz **Załącznik 02 Rejestr podmiotów zewnętrzny**ch.
2. Administrator Danych powierza do przetwarzania dane osobowe będące w jego obszarze fizycznym podmiotom zewnętrznym w oparciu o umowę poufności (**Załącznik 03 Umowa o poufności**). Podmiot zewnętrzny zobowiązany jest do zachowania poufności powierzonych danych i przetwarzania ich zgodnie z celem umowy.
3. Administrator Danych powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę powierzenia przetwarzania danych (**Załącznik 04 Umowa powierzenia**)
    a. Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych.
    b. Podmiot zewnętrzny zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024)

8. Procedura korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI-Administratora Systemu Informatycznego) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji auto uzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą „https:”

9. Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
7. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
8. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
9. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
10. Użytkownicy powinni okresowo kasować niepotrzebne maile. Nie dopuszczalne jest przechowywanie jako załączników w poczcie elektronicznej ważnych dokumentów, dokumentów z danymi osobowych.
11. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.

10. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Procedura opisuje zasady upoważniania osób do przetwarzania danych osobowych oraz zarządzania uprawnieniami użytkowników systemów informatycznych. Celem procedury jest minimalizacja ryzyka przetwarzania danych oraz utraty poufności przez osoby nieupoważnione.

10.1. Zarządzane uprawnieniami użytkowników

1. Przyznanie, anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym wraz z uprawnieniami do przetwarzania tych danych realizowane jest na pisemne zlecenie Dyrektora jednostki lub kierownika po uprzednim zleceniu przez Dyrektora jednostki. Upoważnienie przekazywane jest Administratorowi Bezpieczeństwa Informacji (**Załącznik 05 Upoważnienie do przetwarzania danych osobowych**).
2. Przed nadaniem upoważnienia, ABI zobowiązany jest do sprawdzenia, czy osoba upoważniona:
    a. Odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z Polityką Bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym.
    b. Podpisała oświadczenie o zachowaniu poufności.
    c. Będzie przetwarzać dane osobowe w zakresie i celu określonym w upoważnieniu.
3. ABI jest zobowiązany do aktualizacji upoważnień i ich zakresu (np. z powodu zatrudnienia, urlopu, dostępu do zbiorów lub zmiany stanowiska pracy).
4. Jeśli jest to wymagane, przełożony określa dla osoby upoważnionej jej zakres uprawnień w systemach informatycznych wg. **Załącznika 05a –Zlecenie modyfikacji uprawnień.**
5. Po akceptacji upoważnienia, ABI przekazuje go Informatykowi (ASI) celem nadania identyfikatora oraz uprawnień użytkownika w systemach informatycznych i aplikacjach.
6. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login) i hasło.
7. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie
8. ASI zobowiązany jest po realizacji zlecenia przekazać uzupełniony formularz upoważnienia do ABI.
9. ABI odpowiada za przechowywanie i aktualizację wszystkich upoważnień.
10. ABI odpowiada za prowadzenie rejestru **Załącznik 06 Ewidencja osób upoważnionych do przetwarzania Danych Osobowych**

10.2. Zarządzanie uprawnieniami administratorów

1. Administratorów systemów informatycznych (tzw. Użytkowników uprzywilejowanych) powołuje pisemnie Dyrektor na podstawie załącznika **Załącznik 07 Uprawnienia administratora**.
2. Jeżeli jest to możliwe, każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. „root" lub „admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
3. Jeżeli jest to możliwe, każdy Administrator systemu powinien pracować na koncie administratora przypisanym mu osobiście.

11. Metody i środki uwierzytelnienia

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

11.1. Ogólne zasady postępowania z hasłami

1. ASI informuje mailem/ustnie/telefonicznie użytkownika o nadaniu pierwszego hasła do systemu.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
6. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

11.2. Hasła użytkowników do sieci i serwera

1. Hasło dostępu do sieci składa się co najmniej z 8-miu znaków alfanumerycznych z uwzględnieniem małych i dużych liter.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych
3. Zmiana hasła odbywa się raz na 30 dni
4. Zmiana hasła jest wymuszana przez system / Użytkownicy są zobowiązani do samodzielnej zmiany hasła

11.3. Hasła do programów przetwarzających dane osobowe

1. Hasło dostępu do programu składa się co najmniej z 8-miu znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.
4. Zmiana hasła jest wymuszana przez system.

11.4. Hasła administratora

1. Hasło administratora składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Hasło powinno być znane tylko administratorowi **08 Metryka hasła**) Metryka hasła powinna zawierać: treść hasła, datę jego wprowadzenia do systemu, datę i powód awaryjnego udostępnienia hasła oraz być przechowywane przez okres 5 lat
4. Administrator zobowiązany jest do umieszczenia haseł administratora w zamkniętych kopertach w zamykanej szafie.
5. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

6. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Dyrektora lub Głównego Informatyka osobie zastępującej administratora.
7. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

12. 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.

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabrania się pracy wielu użytkowników na wspólnym koncie.
2. Użytkownik jest zobowiązany do powiadomienia ASI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. „Polityka czystego ekranu”.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 3 minut system automatycznie aktywuje wygaszacz.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

13. Procedura tworzenia kopii zapasowych

13.1. Tworzenie kopii bezpieczeństwa programu Kadrowo – płacowego, finansowo-księgowego.

1. Kopie zapasowe danych kadrowo-płacowych i finansowo-księgowych, tworzone są przez upoważnionego użytkownika lub ASI.
2. Kopie całościowe sporządzane są raz w miesiącu a kopie przyrostowe raz dziennie.
3. Kopie sporządzane są na płytach DVD (1 płyta miesięczna i 4 tygodniowe)

4. Każda płyta jest opisana datą jej sporządzenia. Wszystkie są zaewidencjonowane w „Rejestrze nośników komputerowych zawierających dane osobowe” stanowiącym **Załącznik nr 09** do niniejszej Instrukcji.
5. Kopie całościowe przechowywane są przez 5 lat, a kopie przyrostowe przez 1 miesiąc.
6. Dostęp do kopii mają: Dyrektor, ABI, ASI.
7. Kopie przechowywane są w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu dyrekcji
8. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność poprzez odtworzenie w środowisku testowym.
9. Niszczenie kopii bezpieczeństwa odbywa się poprzez ich zniszczenie w specjalnej niszczarce do CD lub ręcznie.

13.2. Tworzenie kopii bezpieczeństwa dokumentacji serwera

1. Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o specjalne oprogramowanie lub wykorzystanie programowej funkcji serwera.
2. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu (np. w katalogu C:/Operacyjne/).
3. Kopie całościowe sporządzane są raz w miesiącu a kopie przyrostowe raz dziennie.
4. Kopie sporządzane są na wydzielonym twardym dysku wymiennym na komputerze w pomieszczeniu zewnętrznej serwerowni UM (do czasu zaadoptowania innego rozwiązania).
5. Dodatkowo – raz w miesiącu sporządzane są całościowe kopie miesięczne na streamerze.
6. Kopie całościowe przechowywane są przez okres 5 lat a kopie przyrostowe przez 1 miesiąc.
7. Kopie przechowywane są w zabezpieczonym pomieszczeniu.
8. Dostęp do kopii mają: Dyrektor, ABI, ASI.
9. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

14. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków.

14.1. Zabezpieczenie elektronicznych nośników informacji

1. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Zabrania się wynoszenia poza obszar organizacji wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrive bez zgody ADO.
3. Dane osobowe wynoszone poza obszar dokumentacji na nośnikach elektronicznych muszą być zaszyfrowane.

4. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
    c. stosować bezpieczne koperty depozytowe,
    d. przesyłkę należy przesyłać przez kuriera lub dostarczyć samodzielnie.
5. Osoby wykorzystujące nośniki zobowiązane są do niezwłocznego i trwałego (bezzwrotnego) usuwania (kasowania) danych osobowych po ustaniu celu ich przechowywania (chyba, że z powodu odrębnych przepisów należy dane zachowywać).
6. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny w/g **Załącznika 10 Protokół zniszczenia uszkodzonych nośników**.
7. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych/laptopów).
8. Osoby wykorzystujące elektroniczne nośniki z danymi osobowymi są zobowiązane do zabezpieczeniach ich (w szafach, biurkach) przed dostępem osób nieupoważnionych, szczególnie poza godzinami pracy (tzw. „Polityka czystego biurka").

14.2. Zabezpieczenie kopii zapasowych

Zabezpieczenie kopii zapasowych opisane jest w procedurach tworzenia kopii zapasowych.

14.3. Zabezpieczenie dokumentów i wydruków

1. Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
2. Pracownicy są zobowiązani do zabezpieczania dokumentów (np. poprzez zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. „Polityka czystego biurka").
3. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
4. Niszczenie dokumentów zawierających dane osobowe, w tym wydruków tymczasowych musi odbywać się z użyciem niszczarek.
5. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy właściwych jednostek lub komórek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

15. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

15.1. Ochrona antywirusowa

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe

1. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
2. System antywirusowy zainstalowano na serwerze, na stacjach roboczych.
3. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej.
4. Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.
5. Użytkownicy systemu zapewniają stałą aktywność programu antywirusowego, tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
6. Aktualizacja definicji wirusów odbywa się (automatycznie przez system). W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI

15.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.
2. Stosowany jest Firewall programowy na serwerze oraz na stacjach roboczych.

3. Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:
    - Blokowanie stron internetowych określonego typu.
    - Blokowanie określonych stron internetowych.
    - Analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

16. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    a. osoby, której dane dotyczą,

   b. osoby, upoważnionej do przetwarzania danych,
   c. administratora mającego siedzibę w państwie trzecim,
   d. podmiotu, któremu powierzono przetwarzanie danych,
   e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:
   a. nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane
   b. zakresu udostępnianych danych
   c. daty udostępnienia
3. Dane osobowe udostępnia się Odbiorcy danych na pisemny wniosek ze wskazaniem przez Odbiorcę podstawy prawnej legalizującej przetwarzanie DO, z Art. 23 lub Art. 27 UODO.
4. Zgody na udostępnienie danych udziela ABI.
5. Odnotowanie informacji o udostępnieniu danych (komu, zakresie, dacie) powinno nastąpić niezwłocznie po udostępnieniu danych:
   a. w systemie informatycznym, jeśli przetwarza udostępnione dane osobowe,
   b. w postaci ewidencji udostępniania danych (patrz **Załącznik 11 Ewidencja udostępniania danych osobowych**).
6. ABI odpowiada za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.
7. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego, a raport przekazywany jest tej osobie.

17. Procedura wykonywania przeglądów i konserwacji

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

17.1. Przeglądy i konserwacje systemu informatycznego i aplikacji

1. ASI odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych.
2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
5. ASI odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty email.
6. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
8. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
9. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:
    a. wymontować nośniki z danymi osobowymi,
    b. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
    c. nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika,

17.2. *Aktualizacje oprogramowania*

1. ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack, poprawki systemowe).
2. ADO oraz ASI odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

17.3. *Dziennik administratora*

1. ASI dokumentuje pracę w specjalnym rejestrze (patrz **Załącznik 12 Dziennik administratora**)