Załącznik do
Polityki Ochrony Danych Osobowych
w Miejskim Ośrodku Pomocy Rodzinie w Słupsku
z dn.09.09.2024 r.

Polityka zarządzania systemem informatycznym

w
Miejskim Ośrodku Pomocy Rodzinie w Słupsku

Wersja 1		**Pieczęć firmowa:**	
Opracował:	**data**	**Zatwierdził:**	**data**
Piotr Szumko	06.09.2024 r.	DYREKTOR Miejskiego Ośrodka Pomocy Rodzinie w Słupsku Marcin Trader	09.09.2024 r.

1. Wstęp

Polityka stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.

2. Definicje

1. **MOPR** – rozumie się przez to Miejski Ośrodek Pomocy Rodzinie w Słupsku;
2. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Miejskim Ośrodku Pomocy Rodzinie w Słupsku;
3. **Administrator Danych Osobowych (ADO)** –Miejski Ośrodek Pomocy Rodzinie w Słupsku reprezentowany przez Dyrektora MOPR, decydującego o celach i środkach przetwarzania danych osobowych,
4. **Inspektor Ochrony Danych (IOD)** – osoba odpowiedzialna za organizację ochrony danych osobowych;
5. **Administrator Systemu Informatycznego (ASI)** – osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
6. **RODO** - Rozporządzenie 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);
7. **Ustawa** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz.1000);
8. **KRI** - rozumie się przez to ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
9. **Dane osobowe (dane)** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
10. **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;
11. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
12. **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
13. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
14. **Przetwarzanie danych** - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
15. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16. **Dziedzinowy system informatyczny** – samodzielny i niezależny system informatyczny stworzony do świadczenia ściśle określonych usług , nie stanowi on

części innego systemu dziedzinowego, ale może być producentem i konsumentem informacji dla innych systemów dziedzinowych;

17. **Użytkownik** - pracownik Miejskiego Ośrodka Pomocy Rodzinie w Słupsku posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
18. **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
19. **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, pendrivy;
20. **Incydent** - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
21. **Zagrożenie** – potencjalna możliwość wystąpienia incydentu;
22. **Korekcja** – działanie w celu wyeliminowania skutków incydentu;
23. **Działanie korygujące** – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;
24. **Działanie zapobiegawcze** – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej;
25. **Kontrola** – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki i Polityki.

3. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

Szczegółowy opis zabezpieczeń infrastruktury informatycznej i telekomunikacyjnej jest opisane w *załączniku 1 „Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej w MOPR"*

4. Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem loginu i hasła użytkownika.
2. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
3. Zastosowano mechanizm blokady dostępu po 6 próbach nieudanego logowania się.
4. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
5. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.

6. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
7. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
8. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
9. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po **30** minutach).
10. Zastosowano system antywirusowy ESET na stanowiskach, na których przetwarzane są dane osobowe.

5. Procedura korzystania z komputerów przenośnych (laptopów)

Procedura określa zasady korzystania z komputerów przenośnych (laptopów) – *załącznik 2 Regulamin użytkowania komputerów przenośnych (laptopów) w MOPR.*

6. Procedura korzystania z zewnętrznych nośników danych

1. Zewnętrzne nośniki danych użytkowane w MOPR muszą być trwale oznaczone.
2. Użytkownik zobowiązany jest do korzystania z zewnętrznych nośników danych (dyskietki, pendirve, dyski przenośne, itp.) wyłącznie w celach służbowych.
3. Zabrania się użytkowania zewnętrznych nośników danych bez pisemnej zgody (w formie papierowej lub elektroniczne) Dyrektora MOPR.
4. Domyślnie wszystkie nośniki zewnętrzne są blokowane przez system informatyczny. Odblokowanie następuje po uzyskaniu pozwolenia Dyrektora MOPR.

7. 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 ADO i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, 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:".

8. Procedura korzystania z poczty elektronicznej

1. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
2. 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.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
5. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
6. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
7. Użytkownicy powinni okresowo kasować niepotrzebne maile.
8. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".

9. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Procedura opisuje zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty poufności przez osoby nieupoważnione.

9.1. Zarządzane uprawnieniami użytkowników

1. Przyznanie, anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym wraz z uprawnieniami do przetwarzania tych danych realizowane jest na pisemne zlecenie (w formie elektronicznej lub papierowej) ADO Miejskiego Ośrodka Pomocy Rodzinie w Słupsku. Upoważnienie przekazywane jest IOD (patrz *załącznik nr 5_2* do Polityki bezpieczeństwa przetwarzania danych osobowych w MOPR Słupsk - *Upoważnienie do przetwarzania danych osobowych*
2. Przed nadaniem upoważnienia, IOD zobowiązany jest do sprawdzenia, czy osoba upoważniona:
    a. odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z polityką ODO oraz podpisała oświadczenie o odbyciu szkolenia,
    b. podpisała oświadczenie o zachowaniu poufności,
    c. będzie przetwarzać dane osobowe w zakresie i celu określonym upoważnieniu.
3. IOD jest zobowiązany do aktualizacji upoważnień i ich zakresu (np. z powodu zatrudnienia, urlopu, dostępu do zbiorów lub zmiany stanowiska pracy).

4. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
5. IOD odpowiada za przechowywanie i aktualizację wszystkich Upoważnień.
6. IOD opowiada za prowadzenie rejestru wg *załącznika nr 5_3* do Polityki Bezpieczeństwa Ochrony Danych Osobowych w MOPR Słupsk - *Ewidencja osób upoważnionych do przetwarzania danych osobowych w MOPR Słupsk.*

9.2. Zarządzanie uprawnieniami administratorów

1. Administratorów dziedzinowych systemów informatycznych (tzw. Użytkowników uprzywilejowanych) wyznacza Dyrektor MOPR Słupsk na podstawie wniosku IOD. Ewidencja administratorów systemów dziedzinowych jest prowadzona na bieżąco na podstawie *załącznika nr 3 Ewidencja administratorów systemów dziedzinowych.*
2. 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. Hasło „root" znane jest tylko administratorowi odpowiedzialnemu za dany system.
4. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Dyrektora MOPR Słupsk osobie zastępującej administratora.
5. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

10. Metody i środki uwierzytelnienia

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

10.1. Ogólne zasady postępowania z hasłami

1. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany hasła po pierwszym logowaniu (system sam wymusza tę zmianę).
2. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
3. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
4. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

10.2. Hasła do sieci i serwera

1. Hasło dostępu do serwera składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.

10.3. Hasła do programów przetwarzających dane osobowe

1. Hasło dostępu do programów dziedzinowych wykorzystywanych przez MOPR Słupsk składa się co najmniej z 8 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 i jest wymuszana przez system informatyczny (MS Windows oraz systemy dziedzinowe).
5. ASI zobowiązany jest do umieszczenia haseł administratora domeny w zamkniętej kopercie, w kasie pancernej w pok. 14.

10.4. Hasła administratorów systemów dziedzinowych

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.

11. 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.
2. Użytkownik jest zobowiązany do powiadomienia IOD 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 IOD lub 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 **10 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.

12. Procedura tworzenia kopii zapasowych

12.1. Tworzenie kopii bezpieczeństwa dokumentacji serwera

1. Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o oprogramowanie do tworzenia kopii bezpieczeństwa.
2. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narządzi programowych służących do ich przetwarzania w Miejskim Ośrodku Pomocy Rodzinie w Słupsku są opisane w *załączniku nr 4 - Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narządzi programowych służących do ich przetwarzania w Miejskim Ośrodku Pomocy Rodzinie w Słupsku.*
3. Zakres archiwizowanych danych jest określony w *załączniku nr 4_1 Dane komputerowe podlegające archiwizacji w Miejskim Ośrodku Pomocy Społecznej w Słupsku.*
4. Dostęp do kopii mają: IOD, ASI.
5. IOD sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

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

Procedura określa sposób postępowania z nośnikami: twardymi dyskami, płytami CD/DVD, pendrive'ami, telefonami komórkowymi, pamięciami typu „flash" na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

13.1. 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 bez pisemnej zgody (w formie elektroniczne lub papierowej) Dyrektora MOPR.
3. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji 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 stosować bezpieczne koperty depozytowe,
   e. przesyłkę należy przesyłać przez kuriera,
   f. adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).

Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny w/g *załącznika nr 5 do Polityki zarządzania systemem w Miejskim Ośrodku Pomocy Rodzinie w Słupsku - Protokół zniszczenia uszkodzonych nośników komputerowych.*

5. 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 przetwarzania danych MOPR Słupsk (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów).

13.2. 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. 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. Pracownicy są zobowiązani do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
5. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy właściwych jednostek lub komórek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

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

14.1. 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 IOD , 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. ASI pod nadzorem IOD zapewnia 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.
7. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić pisemnie (w formie elektronicznej lub papierowej) ASI lub IOD.

14.2. 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 IOD.
2. Stosowany jest UTM (IPS, IDS, FIREWALL) na styku sieci LAN z Internetem.
3. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: technika NAT.

15. Procedura wykonywania przeglądów i konserwacji

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

15.1. Przeglądy i konserwacje systemu informatycznego i aplikacji

1. ASI odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.
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.

15.2. *Aktualizacje oprogramowania*

1. ASI pod nadzorem IOD odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa nowych wersji (np. aktualizacje, service pack-i, łatki).
2. ASI pod nadzorem IOD odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.