Procedury zarządzania dostępem do systemu przetwarzania danych osobowych

Miejska i Gminna Biblioteka Publiczna im. ks. Jana Twardowskiego w Strzelinie

ul. Grahama Bella 3a
57-100 Strzelin

Dokument do użytku służbowego.
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 02.11.2020 r.

Spis treści

Zasady dotyczące dostępu do systemu przetwarzania danych osobowych

1. Dostęp do systemu przetwarzania danych osobowych w Miejskiej i Gminnej Bibliotece Publicznej im. ks. Jana Twardowskiego w Strzelinie może uzyskać wyłącznie osoba upoważniona do przetwarzania danych przez Administratora Danych Osobowych. Dotyczy to zarówno dostępu do systemu tradycyjnego (kartotek, ksiąg, skorowidzów, akt osobowych, wykazów itp.), jak i systemu informatycznego. Wzór upoważnienia stanowi **Załącznik nr 1** do „Procedur zarządzania dostępem do systemu przetwarzania". Wszystkie osoby upoważnione do przetwarzania danych osobowych ujęte są w wykazie, który prowadzi i aktualizuje Inspektor Ochrony Danych. Wykaz stanowi **Załącznik nr 2** do „Procedur zarządzania dostępem do systemu przetwarzania".
2. Dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, może uzyskać wyłącznie osoba upoważniona do przetwarzania przez Administratora Danych Osobowych i zarejestrowana jako użytkownik w systemie informatycznym przez Administratora Systemu Informatycznego na podstawie ustnego polecenia nadania/odebrania uprawnień w systemie informatycznym.
3. Każdy upoważniony do przetwarzania pracownik, a także każda upoważniona osoba, zatrudniona w bibliotece na innej podstawie niż stosunek pracy (np. umowy zlecenia), również stażysta lub praktykant, przed przystąpieniem do systemu przetwarzania jest zobowiązana odbyć szkolenie, zapoznać się z zasadami ochrony danych osobowych opisanymi w niniejszej dokumentacji oraz podpisać oświadczenie o zachowaniu poufności. Oświadczenie zawarte jest w „Upoważnieniu do przetwarzania danych osobowych" (**Załącznik nr 1** do „Procedur zarządzania dostępem do systemu przetwarzania").
4. Osoba upoważniona do przetwarzania danych osobowych może je przetwarzać wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych, tylko w celu wykonywania nałożonych na nią obowiązków.
5. Zakres dostępu do zbiorów danych osobowych w systemie informatycznym biblioteki przypisany jest do unikatowego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie.
6. Pracownicy biblioteki nieupoważnieni do przetwarzania danych osobowych, wykonujący prace techniczne, porządkowe i konserwatorskie są zobowiązani do podpisania oświadczenia o zachowaniu poufności (**Załącznik nr 3** do „Procedur zarządzania dostępem do systemu przetwarzania").
7. W przypadku konieczności dostępu do obszaru przetwarzania osób nieupoważnionych (niebędących pracownikami biblioteki), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują one oświadczenie o zachowaniu poufności (**Załącznik nr 3**), chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.
8. Firmy wykonujące na rzecz biblioteki prace zlecone, zobowiązane są do zapewnienia środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych, a pracownicy tych firm muszą się stosować do zasad ochrony danych osobowych w nich obowiązujących.

Obszar przetwarzania danych osobowych

W Miejskiej i Gminnej Bibliotece Publicznej im. ks. Jana Twardowskiego w Strzelinie dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania znajdujących się w siedzibie placówki.

Obszarami przetwarzania danych osobowych w placówce ustanowiono wszystkie pomieszczenia, w których dane osobowe zarówno w formie papierowej jak i elektronicznej są tworzone, gromadzone i przechowywane w okresie bieżącego przetwarzania, jak i w postaci archiwów zawartych na nośnikach informatycznych, wydrukach, kartotekach, rejestrach itp.

Obszar przetwarzania danych osobowych w Placówce obejmuje pomieszczenia takie jak: gabinet dyrektora, pokój księgowej, wypożyczalnie i czytelnie dla dorosłych i dzieci, pokój do obsługi czytelników niepełnosprawnych, pokój pracy bibliotekarzy, filię biblioteczną w Nowolesiu. Obszar przetwarzania natomiast nie obejmuje ciągów komunikacyjnych, takich jak korytarze, schody i hole oraz pomieszczeń sanitarno-higienicznych, pomieszczeń socjalnych, gospodarczych i szatni.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

Procedura rozpoczęcia pracy w systemie informatycznym

1. Użytkownik systemu rozpoczynający pracę zobowiązany jest do sprawdzenia zabezpieczeń fizycznych pomieszczenia, a także ogólnego stanu sprzętu informatycznego oraz miejsca przechowywania nośników zawierających dane osobowe. W przypadku zauważenia jakichkolwiek nieprawidłowości w działaniu sprzętu informatycznego lub oprogramowania użytkownik zobowiązany jest niezwłocznie zgłosić ten fakt Administratorowi Systemu Informatycznego.
2. Rozpoczęcie pracy na stacji roboczej następuje po wprowadzeniu indywidualnego identyfikatora oraz hasła, mając na uwadze, iż po przekroczeniu określonej liczby prób logowania, dany system informatyczny blokuje dostęp do zbiorów danych na poziomie użytkownika. Użytkownik powinien poinformować o tym zdarzeniu Administratora Systemu Informatycznego.
3. Logowanie się oraz praca na innych stanowiskach niż indywidualne stanowisko komputerowe użytkownika, wymaga zgody Administratora Danych Osobowych i jest dozwolone jedynie w sytuacjach wyjątkowych.
4. Użytkownik w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym ma obowiązek:
   - ustawienia monitorów w pomieszczeniach w sposób uniemożliwiający osobom nieupoważnionym podgląd,
   - zapewnienia, aby w obszarach przetwarzania danych osobowych osoby nieupoważnione nie przebywały bez nadzoru osoby upoważnionej.

Procedura zawieszenia pracy w systemie informatycznym

W przypadku konieczności zawieszenia pracy w systemie informatycznym z powodu tymczasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest do:

- aktywowania wygaszacza ekranu, zabezpieczonego hasłem,
- wylogowania się z systemu w przypadku, kiedy przerwa w pracy trwa dłużej niż 30 minut,
- niepozostawiania bez nadzoru nośników informacji zawierających dane osobowe - dotyczy to także okresu po zakończeniu pracy (obowiązuje tzw. zasada „czystego biurka" i „czystego ekranu").

Procedura zakończenia pracy w systemie informatycznym

Przed zakończeniem pracy w systemie informatycznym użytkownik zobowiązany jest:

- zapisać wszelkie zmiany w otwartych aplikacjach,
- wykonać kopie zapasowe, jeżeli jest to przewidziane w dokumentacji systemu,
- zamknąć wszystkie używane programy,
- sprawdzić, czy w urządzeniach nie pozostały wymienne elektroniczne nośniki informacji,
- wyłączyć urządzenia peryferyjne (drukarka, skaner itp.),
- wylogować się i zamknąć system,
- sprawdzić, czy pozostawione stanowisko nie stwarza jakichkolwiek zagrożeń i czy jest prawidłowo zabezpieczone przed uruchomieniem przez osoby postronne.

Metody uwierzytelnienia użytkowników w systemie informatycznym

W Miejskiej i Gminnej Bibliotece Publicznej im. ks. Jana Twardowskiego w Strzelinie system informatyczny, w którym przetwarza się dane osobowe, wyposażony jest w mechanizmy uwierzytelniania użytkowników przy pomocy identyfikatora i hasła.

Po zalogowaniu się do systemu informatycznego dostęp do poszczególnych programów, baz danych i aplikacji, w których przetwarzane są dane osobowe (ALEPH - zintegrowany system biblioteczny umożliwiający elektroniczny dostęp on-line czytelników do zasobów biblioteki, Comarch ERP Optima, Płatnik), jest możliwy po dokonaniu uwierzytelnienia również za pomocą identyfikatora i hasła, i powinien przebiegać zgodnie z instrukcją zawartą w dokumentacji programu/aplikacji.

Identyfikator użytkownika

1. Każdy użytkownik systemu informatycznego posiada swój unikatowy identyfikator.
2. Użytkownicy nie mogą używać tych samych identyfikatorów ani wymieniać się nimi.
3. Identyfikator po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
4. Kontrolę nad powyższymi czynnościami sprawuje Administrator Systemu Informatycznego.

Hasło użytkownika

1. Hasło dostępu ustala dla siebie użytkownik.
2. Hasło dostępu powinno składać się z unikatowego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.
3. W systemie informatycznym zmiana haseł dostępu powinna następować co najmniej co 30 dni.
4. Za zmianę hasła odpowiada użytkownik.
5. Użytkownik niezwłocznie zmienia hasło w przypadku podejrzenia lub stwierdzenia: podglądu, przechwycenia, podsłuchania lub odgadnięcia.
6. Użytkownik zobowiązany jest do utrzymania hasła dostępu w tajemnicy zarówno w czasie zatrudnienia, jak też po jego ustaniu.
7. W sytuacji udostępnienia hasła innej osobie, użytkownik ponosi odpowiedzialność za skutki i następstwa wynikłe z faktu wykorzystania tego hasła przez osoby trzecie.
8. W przypadku zastosowania awaryjnego dostępu do systemu informatycznego na poziomie użytkownika (zapomniane hasło, blokada dostępu), Administrator Systemu Informatycznego nadpisuje hasło użytkownika za pomocą nowego hasła początkowego, po dokonaniu uprzedniej weryfikacji tożsamości użytkownika.
9. Hasła dostępu wyświetlane są na ekranie monitora w formie niedającej się odczytać osobom postronnym i mogą być znane tylko użytkownikowi.

Hasło Administratora Systemu Informatycznego

1. Hasła Administratora Systemu Informatycznego przechowywane są w postaci klasycznego zapisu w zabezpieczonej kopercie lub na elektronicznych nośnikach informacji CD-ROM (jednokrotnego zapisu), w postaci odpowiednio zabezpieczonego pojedynczego pliku w bezpiecznym miejscu wyznaczonym przez dyrektora.
2. W sytuacjach awaryjnych lub w razie nieobecności Administratora Systemu Informatycznego jego zadania spoczywają na osobach upoważnionych przez dyrektora. W przypadku wykorzystania haseł podczas nieobecności Administratora Systemu Informatycznego, muszą one być niezwłocznie zmienione po wznowieniu wykonywania obowiązków przez ASI.

Procedury nadawania, rejestrowania i odbierania uprawnień w systemie informatycznym

Nadanie uprawnień w systemie

1. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadawane są wyłącznie pracownikom, którzy uzyskali upoważnienie do przetwarzania danych osobowych.
2. Zakres dostępu do danych przetwarzanych w systemie nie może być większy niż w wydanym wcześniej upoważnieniu.
3. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadawane są na polecenie Administratora Danych Osobowych (dyrektora) przez Administratora Systemu Informatycznego.

4. Przydzielenie użytkownikowi uprawnień do przetwarzania danych w systemach informatycznych jest jednoznaczne z nadaniem mu loginu oraz hasła tymczasowego.
5. Administrator Systemu Informatycznego przekazuje użytkownikowi jego identyfikator i hasło inicjujące pracę w systemie informatycznym. Użytkownik, po otrzymaniu informacji o założonym koncie z wymaganymi uprawnieniami:
   - loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,
   - przy pierwszym logowaniu zmienia nadane mu przez Administratora Systemu hasło.
6. Administrator Systemu Informatycznego prowadzi rejestr nadanych uprawnień w systemach informatycznych.

Odebranie uprawnień w systemie

1. Na polecenie Administratora Danych Osobowych Administrator Systemu Informatycznego odbiera uprawnienia użytkownika w systemach informatycznych.
2. Użytkownika wyrejestrowuje się z systemu w sytuacji ustania jego zatrudnienia lub długotrwałej nieobecności w pracy.
   - Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik. Rozwiązanie umowy o pracę powoduje utratę dostępu użytkownika do systemu informatycznego oraz do całego systemu przetwarzania danych.
   - Podstawą czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
     - nieobecność użytkownika w pracy trwająca dłużej niż 30 dni kalendarzowych,
     - zawieszenie w pełnieniu obowiązków służbowych,
     - wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych.

Zmiana danych identyfikacyjnych użytkownika

W przypadku zmiany danych identyfikacyjnych użytkownika Administrator Systemu Informatycznego dokonuje zmian w systemie informatycznym polegających na wyrejestrowaniu i ponownym zarejestrowaniu użytkownika ze zmienionymi danymi identyfikacyjnymi oraz nadaniu mu nowego identyfikatora i hasła inicjującego pracę w systemie, na podstawie polecenia Administratora Danych Osobowych.

Zmiana zakresu dostępu użytkownika

W przypadku zmiany zakresu dostępu użytkownika Administrator Systemu Informatycznego dokonuje zmian w systemie informatycznym polegających na wyrejestrowaniu i ponownym zarejestrowaniu użytkownika ze zmienionym zakresem dostępu oraz nadaniu mu nowego hasła inicjującego pracę w systemie, na podstawie polecenia Administratora Danych Osobowych. W przypadku zmiany zakresu dostępu, identyfikator użytkownika nie ulega zmianie.

Sposoby zabezpieczenia systemu informatycznego przed działaniem szkodliwego oprogramowania

1. Obszarami systemu informatycznego narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są m. in.: dysk twardy urządzenia, pamięć RAM, elektroniczne nośniki informacji np. płyty CD /DVD, pamięci USB.
2. Drogą przedostania się wirusów i szkodliwego oprogramowania do systemu mogą być sieci informatyczne, zainfekowane elektroniczne nośniki danych oraz załączniki poczty e-mail, pochodzące od nieznanych nadawców.
3. W celu zabezpieczenia przed atakami z sieci publicznej serwery i stacje robocze znajdujące się w sieciach LAN są chronione przez zaporę ogniową (firewall).
4. Na wszystkich stacjach roboczych i serwerach pracujących pod kontrolą systemu operacyjnego Microsoft Windows zainstalowany jest program antywirusowy.
5. Oprogramowanie antywirusowe sprawuje ciągły nadzór nad uruchamianymi lub wprowadzanymi do systemu programami oraz załącznikami poczty elektronicznej.
6. Za zabezpieczenie systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego odpowiada Administrator Systemu Informatycznego.
7. Użytkownicy systemu poddawani są szkoleniom co do stosowania zasad bezpieczeństwa danych w ramach wewnętrznych szkoleń adaptacyjnych:
   - z zasad bezpiecznej pracy pozwalających unikać szkodliwego oprogramowania,
   - z zasad postępowania w przypadku wykrycia lub podejrzenia działania złośliwego oprogramowania (osobą odpowiedzialną za przeprowadzanie szkoleń w powyższym zakresie jest dyrektor, powierzając do zadanie Administratorowi Systemu Informatycznego).

Zasady korzystania z Internetu, poczty elektronicznej i oprogramowania

Zasady bezpiecznego użytkowania systemu informatycznego

1. Zabrania się użytkownikowi podłączania do systemu informatycznego nieautoryzowanych (prywatnych) nośników informacji. Do komputera można podłączać jedynie służbowe nośniki służące do przenoszenia danych lub tworzenia kopii zapasowych.
2. Zabrania się użytkownikowi przechowywania na służbowym komputerze jakichkolwiek materiałów niezwiązanych z wykonywanymi obowiązkami służbowymi. Zabrania się w szczególności przechowywania na służbowym komputerze materiałów naruszających prawa autorskie. Za wszelkie naruszenia praw autorskich związanych z nieuprawnionymi materiałami przechowywanymi lub pobieranymi na komputer służbowy odpowiada użytkownik.
3. Zabrania się podłączania prywatnych komputerów oraz innych urządzeń sieciowych do sieci LAN/WAN. Wymaga to akceptacji Administratora Danych Osobowych. Zabrania się również podłączania służbowych komputerów znajdujących się w obszarze funkcjonowania placówki nieautoryzowanych sieci LAN/WAN za pomocą urządzeń, które nie są częścią systemu informatycznego placówki.

Zasady korzystania z oprogramowania

1. Zabrania się instalowania oraz używania oprogramowania innego niż udostępnione przez dyrektora.
2. Zabrania się kopiowania lub usuwania oprogramowania zainstalowanego w systemie informatycznym placówki.
3. Instalowanie jakiegokolwiek oprogramowania związanego z obsługą urządzeń peryferyjnych wchodzących w skład systemu informatycznego może być dokonane wyłącznie przez Administratora Systemu Informatycznego.

Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu tylko w celach służbowych.
2. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
3. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu rozpoczynającego się frazą „https:”
4. Zabrania się odwiedzania stron o treściach prawnie zabronionych lub powszechnie uznanych za niebezpieczne.
5. Zabrania się pobierania z Internetu plików pochodzących z niewiarygodnych źródeł.

Zasady korzystania z poczty elektronicznej

1. Przesyłanie wiadomości zawierających dane osobowe może odbywać się wyłącznie przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
3. Należy zwrócić szczególną uwagę na poprawność adresu odbiorcy wiadomości.
4. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody UDW (ukryte do wiadomości).
5. Nie należy otwierać wiadomości oraz załączników i linków otrzymanych od nieznanych nadawców. W takiej sytuacji należy skontaktować się z Administratorem Systemu Informatycznego.

Zasady postępowania z elektronicznymi nośnikami informacji zawierającymi dane osobowe

1. Elektroniczne nośniki informacji zawierające dane osobowe na czas ich użyteczności przechowywane są w zamkniętych na klucz szafach/zabezpieczonych meblach biurowych.
2. W przypadku dalszego wykorzystywania w innych celach, nośniki pozbawiane są zapisu danych w sposób uniemożliwiający ich odzyskanie.

3. Elektroniczne nośniki informacji, które zostały przeznaczone do likwidacji, pozbawiane są wcześniej zapisu danych, a w przypadku gdy nie jest to możliwe, uszkadzane w sposób uniemożliwiający ich odczytanie.

Zasady postępowania przy przekazywaniu nośników informacji do innej jednostki organizacyjnej

1. Elektroniczne nośniki informacji zawierające dane osobowe przekazywane są do innej jednostki organizacyjnej tylko na pisemny, umotywowany wniosek, gdy jest to bezwzględnie konieczne do realizacji jej zadań regulaminowych.
2. Pliki z informacjami zawarte na nośnikach przekazywanych poza obszar przetwarzania, obowiązkowo zabezpieczane są przed dostępem osób i podmiotów nieupoważnionych oraz modyfikacją lub zniszczeniem w sposób nieautoryzowany - hasłem dostępu lub szyfrując je.
3. Przed wysłaniem nośnika sporządzana jest kopia przesyłanych danych, a adresat powiadamiany jest o nadanej przesyłce. W przypadku nieotrzymania przez adresata przesyłki, o zaistniałej sytuacji powiadamiany jest Inspektor Ochrony Danych.
4. Elektroniczne nośniki informacji pochodzące od podmiotu zewnętrznego sprawdzane są programem antywirusowym.

Zasady postępowania z komputerami przenośnymi

Użytkownik komputera przenośnego jest zobowiązany do:

- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,
- zabezpieczenia komputera przenośnego hasłem, zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym,
- niezezwalania osobom nieupoważnionym i nieuprawnionym do korzystania z komputera przenośnego,
- korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby postronne, w szczególności zabrania się korzystania z komputera przenośnego w miejscach publicznych i w środkach transportu publicznego.

Procedury zarządzania kopiami zapasowymi

Procedura tworzenia kopii zapasowych

1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora DO zabezpieczane są w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub kopii archiwalnych.
2. Kopie bezpieczeństwa wykonywane są zawsze przed:
   - dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania,
   - dokonaniem zmian w programach (np. zmiana wersji lub aktualizacja oprogramowania),
   - każdą istotną zmianą danych w bazie danych.

3. Jeśli zaistnieje taka konieczność, tworzone są awaryjne kopie zapasowe, np. przed dokonaniem niezbędnych napraw systemu informatycznego bądź komputera, na którym przetwarzane są dane osobowe.
4. Za tworzenie kopii zapasowych przy użyciu narzędzi systemowych i systemów do tego przystosowanych odpowiedzialny jest ASI.

Procedura przechowywania i niszczenia kopii zapasowych

1. Nośniki informacji zawierające kopie zapasowe zbiorów danych osobowych, programów i narzędzi programowych służących do przetwarzania danych osobowych przechowywane są w sposób uniemożliwiający ich nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników z kopiami zapasowymi posiada tylko Administrator Danych Osobowych i Administrator Systemu Informatycznego.
3. Serwisowanie lub naprawy nośników zawierających kopie zapasowe przez osoby, które nie są pracownikami biblioteki, odbywa się wyłącznie pod nadzorem Administratora Systemu Informatycznego.
4. W przypadku braku możliwości naprawy uszkodzonych nośników zawierających kopie zapasowe, przeznacza się je do utylizacji z uzyskaniem potwierdzenia zniszczenia. Z wykonanych czynności sporządza się protokół.

Procedury wykonywania przeglądów i konserwacji systemu informatycznego

1. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji w Miejskiej i Gminnej Bibliotece Publicznej im. ks. Jana Twardowskiego w Strzelinie dokonuje stosownie do potrzeb Administrator Systemu Informatycznego, nie rzadziej niż raz na rok. ASI przynajmniej raz w roku:
   - dokonuje procedury przeglądu zestawów komputerowych będących w użytkowaniu pod kątem występowania usterek sprzętowych,
   - dokonuje przeglądu komputerów czasowo wyłączonych z użytku z powodu usterek, pod kątem możliwości naprawy lub docelowego wycofania z użytku,
   - przeprowadza weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich komputerach podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa.
2. W przypadku stwierdzenia nieprawidłowości w działaniu elementów systemu informatycznego, które są niezbędne do zapewnienia realizacji celów wynikających z dokumentacji ochrony danych osobowych, ASI podejmuje niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania.

Zasady serwisowania sprzętu komputerowego

1. Użytkownik systemu informatycznego niezwłocznie powiadamia Administratora Systemu o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia bezpieczeństwa danych osobowych.
2. O powyższych przypadkach ASI zawiadamia niezwłocznie ADO.
3. Wszystkie awarie lub usterki sprzętowe są zgłaszane w dniu wystąpienia i usuwane na bieżąco.
4. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników systemu napraw sprzętu informatycznego, wymiany jego podzespołów oraz wykonywanie innych czynności niezwiązanych bezpośrednio z jego eksploatacją lub niedopuszczonych przez producenta sprzętu w instrukcji obsługi.
5. W przypadku, gdy do przywrócenia prawidłowego działania systemu informatycznego niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym zawierającym dane osobowe dokonywane są w obszarze przetwarzania danych osobowych wyłącznie w obecności ASI.
6. Zdiagnozowane usterki elementów zestawów komputerowych są:
   - w przypadku objęcia gwarancją - zgłaszane do autoryzowanych serwisów producenta sprzętu w celu naprawy lub wymiany na elementy wolne od wad,
   - w przypadku braku gwarancji - naprawiane przez osoby do tego upoważnione w bibliotece lub przy braku możliwości technicznych oddane do naprawy w serwisach zewnętrznych.
7. W każdym z przypadków, jeżeli w celu dokonania naprawy wymagane jest przekazanie na zewnątrz dysków twardych, ich zawartość jest bezwzględnie archiwizowana i pozbawiana zapisu danych osobowych.

Zasady wycofywania z użytkowania stacji roboczych

1. W każdym przypadku, kiedy uszkodzeniu ulegnie jednostka centralna zestawu komputerowego, monitor lub drukarka, a zestaw komputerowy jako całość lub jego poszczególne elementy nie posiadają ważnej gwarancji, następuje oszacowanie możliwości jak i kosztów naprawy. Jeżeli koszty naprawy przekraczają wartość zakupu nowego elementu składowego lub naprawa jest niemożliwa, przeprowadza się procedurę wycofania takiego elementu z dalszej eksploatacji:
   - sporządza się krótką notatkę o braku możliwości naprawy lub nieopłacalności jej realizacji,
   - zgłasza fakt wycofania sprzętu z użytku osobie odpowiedzialnej za prowadzenie ewidencji ilościowo - wartościowej sprzętu komputerowego,
   - dokonuje wykreślenia ze stanu ewidencyjnego,
   - w przypadku jednostki centralnej, zabezpiecza dysk twardy poprzez jego wymontowanie i pozostawienie w bibliotece lub poddanie procedurze pozbawienia zapisu danych w uprawnionych do tego podmiotach,
   - dokonuje złomowania poprzez przekazanie firmom wyspecjalizowanym w utylizacji nośników.
2. Za powyższe czynności odpowiedzialny jest Administrator Systemu Informatycznego.

Zasady postępowania z dokumentami papierowymi

1. Podczas nieobecności w pomieszczeniu lub po zakończeniu pracy, dokumenty oraz wydruki zawierające dane osobowe przechowane są w szafkach i meblach biurowych zamykanych na klucz.
2. Dokumenty i wydruki oraz kserokopie dokumentów nie są pozostawiane na urządzeniach bez nadzoru.
3. Dokumenty i wydruki, niezwłocznie po ustaniu celu ich przetwarzania, niszczone są w niszczarkach.
4. W przypadku konieczności przekazania poza obszar przetwarzania, dokumenty transportowane są i przekazywane z zachowaniem szczególnej ostrożności przez osobę do tego upoważnioną.

Załączniki

Załącznik nr 1	- Upoważnienie do przetwarzania danych osobowych.
Załącznik nr 2	- Wykaz osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 3	- Oświadczenie o zachowaniu poufności.