**POLITYKA OCHRONY DANYCH**

**Miejskiej Biblioteki Publicznej im. Zdzisława Arentowicza we Włocławku**

wprowadzona Zarządzeniem Dyrektora Miejskiej Biblioteki Publicznej

im. Zdzisława Arentowicza we Włocławku nr 31/2018z dnia 31 grudnia 2018r.,

które weszło w życie z dniem 1 stycznia 2019r.

**Tekst jednolity ogłoszony zarządzeniem nr 10/2024 Dyrektora Miejskiej Biblioteki Publicznej**

**im. Zdzisława Arentowicza we Włocławku z dnia 10 czerwca 2024r.**

*Niniejszy dokument zatytułowany „****Polityka ochrony danych****” (dalej jako* ***Polityka****) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Miejskiej Bibliotece Publicznej im. Zdzisława Arentowicza we Włocławku (dalej jako* ***Biblioteka****).*

*Polityka Ochrony Danych została wydana na podstawie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) (Dz. Urz. UE L 119, s. 1) oraz rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017r. poz. 2247).*

**§ 1. Cele i deklaracje**

1. Dyrektor Biblioteki, świadomy wagi zagrożeń jakie niesie ze sobą przetwarzanie danych osobowych dla wolności i praw osób, których dane dotyczą, uznaje ochronę tych danych, w szczególności zapewnienie ich bezpieczeństwa, za jeden z priorytetów działalności Biblioteki.
2. Dyrektor Biblioteki podejmuje działania mające na celu wdrożenie przez Bibliotekę przepisów o ochronie danych osobowych oraz zapewnienie stałej zgodności działalności Biblioteki z tymi przepisami.
3. W celu realizacji zadań określonych w ust. 1. i 2. ustanawia się niniejszą Politykę Ochrony Danych.
4. Polityka określa w szczególności:
5. sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną;
6. podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
7. wymagania w zakresie odnotowywania udostępnianych danych osobowych oraz bezpieczeństwa ich przetwarzania.
8. Dyrektor Biblioteki oczekuje, że zasady i procedury określone w niniejszym dokumencie będą faktycznie wdrożone i stosowane przez ich adresatów. Zobowiązuje się wszystkie osoby dopuszczone do przetwarzania danych osobowych w Bibliotece do dostosowania ich postępowania do wymogów wynikających z niniejszej Polityki Ochrony Danych.

**§ 2. Zakres stosowania**

1. Zasady i procedury określone w niniejszym dokumencie stosuje się zarówno do danych osobowych przetwarzanych w sposób tradycyjny w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i do danych przetwarzanych w systemach informatycznych, także wtedy gdy dane te przetwarzane są poza zbiorami danych.
2. Zasady i procedury określone w niniejszym dokumencie stosuje się do wszystkich osób przetwarzających dane osobowe w ramach Bibliotece, zarówno do tych zatrudnionych w Bibliotece, jak i innych osób, które zostały dopuszczone do przetwarzania, w szczególności do osób świadczących usługi na podstawie umów cywilnoprawnych oraz wolontariuszy, praktykantów, itd.

**§ 3. Skróty i definicje**

Ilekroć w Polityce Ochrony Danych jest mowa o:

1. RODO – rozumie się przez to Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) (Dz. Urz. UE L 119, s. 1),
2. Ustawie – rozumie się przez to ustawę z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz.U. z 2019r. poz. 1781),
3. Polityce – należy przez to rozumieć Politykę Ochrony Danych Miejskiej Biblioteki Publicznej im. Zdzisława Arentowicza we Włocławku,
4. Administratorze Danych Osobowych – rozumie się przez to Miejską Bibliotekę Publiczną im. Zdzisława Arentowicza we Włocławku reprezentowaną przez Dyrektora,
5. Bibliotece – należy przez to rozumieć Miejską Bibliotekę Publiczną im. Zdzisława Arentowicza we Włocławku,
6. Dyrektorze – należy przez to rozumieć Dyrektora Miejskiej Biblioteki Publicznej im. Zdzisława Arentowicza we Włocławku,
7. Inspektorze Ochrony Danych – rozumie się przez to osobę, której administrator danych powierzył realizację zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych stosownie do właściwych przepisów RODO,
8. Administratorze Systemu Informatycznego – rozumie się przez to osobę zarządzającą i sprawującą bieżący nadzór nad poprawnością działania systemu informatycznego,
9. upoważnionym - rozumie się przez to osobę, która została upoważniona do przetwarzania danych osobowych,
10. użytkowniku – rozumie się przez to upoważnionego, któremu nadano identyfikator i przyznano hasło,
11. podmiocie przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 28 RODO,
12. odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
13. osoby, której dane dotyczą,
14. osoby upoważnionej do przetwarzania danych,
15. przedstawiciela, o którym mowa w art. 27 RODO,
16. podmiotu przetwarzającego, o którym mowa w art. 28 RODO,
17. organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z przepisami prawa,
18. serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,
19. systemie informatycznym Administratora Danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,
20. haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
21. identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
22. uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
23. poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
24. integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione, usunięte lub zniszczone w sposób nieautoryzowany,
25. rozliczalności – rozumie się przez to właściwość zapewniającą, że podejmowane działania mogą być przypisane w sposób jednoznaczny konkretnej osobie lub podmiotowi,
26. raportach – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.

**§ 4. Administrator Danych Osobowych**

Administrator Danych Osobowych reprezentowany przez Dyrektora realizuje zadania
w zakresie ochrony danych osobowych, w tym w szczególności:

1. podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,
2. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków oraz odwołuje przedmiotowe upoważnienia,
3. wyznacza Inspektora Ochrony Danych oraz określa zakres jego zadań i czynności na podstawie art. 37 rozporządzenia 2016/679 i zawiadomienia Prezesa Urzędu o jego wyznaczeniu, w terminie do dnia 31 lipca 2018r. stosownie do art. 158 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000),
4. zleca kierownikom poszczególnych działów, by we współpracy z Administratorem Systemu Informatycznego oraz Inspektorem Ochrony Danych osobowych zapewnili użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych,
5. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

**§ 5. Inspektor Ochrony Danych**

Inspektor Ochrony Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym w szczególności:

1. sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
2. sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń danych osobowych przy współpracy z administratorem systemu,
3. przeprowadza wewnętrzne audyty (sprawdzenia) przestrzegania przepisów o ochronie danych osobowych, aktualności dokumentacji z zakresu ochrony danych osobowych oraz przestrzegania określonych w niej zasad,
4. nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
5. zapoznaje się na bieżąco z przepisami dotyczącymi ochrony danych osobowych i wytycznymi organu nadzorczego w tej dziedzinie, dbając o dostosowanie działalności Biblioteki do aktualnych wymogów prawnych,
6. przygotowuje lub zatwierdza dokumenty lub odpowiednie klauzule w dokumentach dotyczące ochrony danych osobowych,
7. prowadzi lub nadzoruje prowadzenie dokumentacji z zakresu ochrony danych osobowych,
8. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych,
9. nadzoruje realizację obowiązku zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie tych danych, w szczególności decyduje o terminach i sposobach przeprowadzenia szkoleń w tym zakresie.

**§ 6. Administrator Systemu Informatycznego**

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym w szczególności:

1. zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z uprawnieniami administratora,
2. na wniosek pracownika odpowiedzialnego w sprawach kadr przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego i dokonuje ewentualnych modyfikacji uprawnień, a także wyrejestrowuje użytkowników i usuwa ich konta,
3. nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych we współpracy z dostawcą systemu informatycznego służącego do przetwarzania danych osobowych (SOWA SQL),
4. podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
5. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
6. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Inspektora Ochrony Danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
7. prowadzi dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym w oparciu o *Rejestr Naruszeń*, który stanowi *załącznik nr 8 do Polityki*,
8. wykonuje naprawy, konserwuje oraz likwiduje urządzenia komputerowe, na których zapisane są dane osobowe, wykonuje kopie zapasowe, przechowuje je oraz okresowo sprawdza pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego, bądź też nadzoruje wykonywanie tych czynności przez osoby trzecie,
9. aktualizuje oprogramowanie systemowe, chyba że aktualizacje wykonywane są automatycznie,
10. aktualizuje oprogramowanie antywirusowe, chyba że aktualizacje wykonywane są automatycznie,
11. podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
12. realizuje niecierpiące zwłoki zadania Inspektora Ochrony Danych, w przypadku jego nieobecności w Bibliotece.

**§ 7. Pracownik odpowiedzialny w spawach kadr**

Pracownik odpowiedzialny w spawach kadr realizuje następujące zadania w zakresie ochrony danych osobowych:

1. prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
2. prowadzi ewidencję użytkowników systemu informatycznego we współpracy z Administratorem Systemu Informatycznego,
3. występuje z wnioskiem do Administratora Danych Osobowych o nadanie upoważnienia do przetwarzania danych osobowych,
4. występuje z wnioskiem do Administratora Systemu Informatycznego o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych,
5. występuje z wnioskami o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego.

**§ 8. Upoważniony**

Każdy upoważniony do przetwarzania danych:

1. musi mieć imienne upoważnienie nadane przez Administratora Danych Osobowych do przetwarzania danych *(wzór upoważnienia stanowi załącznik nr 4 do Polityki)*,
2. może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w upoważnieniu i tylko w celu wykonywania nałożonych na niego obowiązków, a rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych; zakres dostępu do danych przetwarzanych w systemie informatycznym przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy,
3. musi zachować w tajemnicy treść danych osobowych oraz sposób ich zabezpieczenia przez cały okres zatrudnienia w Bibliotece, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
4. zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych, w tym w szczególności przepisami niniejszej Polityki,
5. składa oświadczenie o zapoznaniu się z przepisami Polityki Ochrony Danych oraz z przepisami o odpowiedzialności karnej za naruszenie ochrony danych osobowych i zachowaniu w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia, także po ustaniu okresu zatrudnienia,
6. stosuje się do wydawanych przez Administratora Danych Osobowych, Inspektora Ochrony Danych oraz innych przełożonych procedur, wytycznych oraz poleceń służbowych mających na celu zapewnienie zgodnego z prawem przetwarzania danych osobowych,
7. korzysta z systemu informatycznego Administratora Danych Osobowych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników oraz stosownie do zaleceń Administratora Systemu Informatycznego,
8. korzysta z systemu informatycznego służącego do przetwarzania danych osobowych tylko w godzinach pracy Biblioteki, a po godzinach pracy – po uprzednim zawiadomieniu przełożonego,
9. zabezpiecza dane przed ich utratą, nieautoryzowanym zmienieniem lub ujawnieniem osobom nieupoważnionym.

**§ 9. Zasoby danych osobowych**

Na zasoby danych osobowych Biblioteki składają się zarówno dane osobowe przetwarzane w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i dane przetwarzane w systemach informatycznych.

**§ 10. Miejsce przetwarzania**

1. Dane osobowe można przetwarzać zgodnie z niniejszym dokumentem w pomieszczeniach Biblioteki do tego przystosowanych.
2. Ze względu na szczególne nagromadzenie danych osobowych, szczególnie chronione są pomieszczenia serwerowni, pomieszczenia w których przechowuje się i składuje kopie zapasowe danych osobowych, pomieszczenia archiwum zakładowego oraz pomieszczenia komórek finansowo - księgowych i kadrowych.
3. Pomieszczenia zabezpiecza się przed dostępem osób trzecich na czas nieobecności osób upoważnionych do przetwarzania danych osobowych.

§ 11. System informatyczny

1. Na System Informatyczny Administratora Danych Osobowych składają się programy opisane w niniejszej Polityce.
2. Na jego opis składają się w szczególności: lokalizacja serwera, zabezpieczenia, połączenie z siecią i stacje robocze.

**§ 12. Programy stosowane do przetwarzania danych**

|  |  |  |
| --- | --- | --- |
| **Programy stosowane do przetwarzania** **danych osobowych** | **Wykaz zbiorów** **danych osobowych** | **Wykaz pomieszczeń,** **w których zbiory danych osobowych są przetwarzane** |
| **COMARCH OPTIMA** | **Dane kadrowe i płacowe** | **Księgowość** |
| **PŁATNIK** | **Dane kadrowe i płacowe** | **Księgowość** |
| **SOWA SQL** | **Dane osobowe użytkowników** | **Serwerownia** |

**§ 13. Lokalizacja systemów informatycznych**

Zbiory wymienione w powyższej tabeli znajdują się:

1. w budynku Miejskiej Biblioteki Publicznej im. Zdzisława Arentowicza we Włocławku przy ul. Warszawskiej 11/13 – COMARCH OPTIMA i PŁATNIK,
2. na serwerach dostawcy systemu informatycznego - SOKRATES-software Leszek Masadyński, ul. Warszawska 92A, 61-047 Poznań – SOWA SQL.

**§ 14. Migracja danych**

1. Przepływ danych odbywa się między programami:
2. COMARCH OPTIMA, a PŁATNIKIEM – wymiana danych niezbędnych do przekazania składek ZUS (dane płacowe) – sieć wewnętrzna,
3. SOWA SQL – dane biblioteczne na zasadzie importu danych.
4. Dane poddawane transmisji z zewnętrznymi serwerami danych zaszyfrowane są za pomocą klucza kwalifikowanego lub za pomocą wewnętrznych procedur szyfrowania danych programów.

**§ 15. Opis sposobu przetwarzania**

1. Sposób przetwarzania danych osobowych w systemie informatycznym administratora danych określają załączniki: *Opis Zasobów Danych Osobowych* oraz *Rejestr Czynności Przetwarzania*.
2. *Opis Zasobów Danych* osobowych Biblioteki obejmuje w szczególności informację o treści i strukturze każdego z zasobów oraz o sposobie przepływu danych pomiędzy.
3. *Rejestr Czynności Przetwarzania* prowadzony jest zgodnie z art. 30 RODO i zawiera co najmniej następujące informacje:
4. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
5. cele przetwarzania,
6. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
10. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. RODO.
11. Dokładny opis techniczny zbiorów danych, wskazujący zawartość poszczególnych pól informatycznych i powiązania między nimi znajduje się w dokumentacji oprogramowania u Administratora Systemów Informatycznych.

§ 16. Dokumentacja ochrony danych osobowych

1. Biblioteka prowadzi dokumentację ochrony danych osobowych na którą składają się:
2. *Opis Obszaru Przetwarzania Danych Osobowych,*
3. *Opis Zasobów Danych Osobowych,*
4. *Rejestr Czynności Przetwarzania,*
5. dokumentacja audytów,
6. umowy z podmiotami przetwarzającymi (jeśli zostaną zawarte),
7. umowy z współadministratorami (jeśli zostaną zawarte).
8. W ramach dokumentacji ochrony danych osobowych prowadzone są następujące ewidencje:
9. pracownik odpowiedzialny w sprawach kadr prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz ewidencję użytkowników systemu informatycznego (we współpracy z Administratorem Systemu Informatycznego),
10. Inspektor Ochrony Danych prowadzi ewidencję udostępnień danych osobowych,
11. Administrator Systemu Informatycznego prowadzi naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym oraz ewidencję użytkowników komputerów przenośnych.
12. Na dokumentację audytów składają się:
13. dokumentacja sprawdzeń planowych,
14. dokumentacja sprawdzeń doraźnych.

§ 17. Identyfikacja zagrożeń bezpieczeństwa danych osobowych

Identyfikuje się następujące zagrożenia bezpieczeństwa danych osobowych przetwarzanych
w Bibliotece:

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej, włamanie do budynku,
2. niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne),
3. awarie sprzętu lub oprogramowania, zarówno losowe, jak i spowodowane przez niewłaściwe działanie użytkowników i serwisantów,
4. zastosowanie niewłaściwych metod zabezpieczenia systemu informatycznego lub brak dostosowania poziomu zabezpieczeń do aktualnego poziomu wyzwań technologicznych,
5. działania przestępcze mające na celu przejęcie lub zniszczenie danych osobowych (np. ataki internetowe),
6. podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych,
7. naruszenia zasad i procedur określonych w dokumentacji ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, będące skutkiem nieprzestrzegania procedur ochrony danych, w tym w szczególności:
8. wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez wiedzy i zgody administratora systemu,
9. ujawnienie osobom nieupoważnionym danych osobowych, jak też procedur ochrony danych stosowanych u Administratora Danych Osobowych (poprzez umożliwienie wglądu lub przekazania danych i dokumentacji),
10. naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie lub zgoda na takie działania przez inne osoby (np. udostępnienie identyfikatora i hasła innemu użytkownikowi),
11. niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na portiernię),
12. przetwarzanie danych osobowych w celach niezgodnych z ich przeznaczeniem.

§ 18. Ograniczenia dostępu do pomieszczeń

1. W siedzibie administratora danych wydzielono pomieszczenia z ograniczonym dostępem:
2. pomieszczenie serwerowni (w którym znajdują się m.in. modem, router, urządzenie ups), w którym mogą przebywać wyłącznie: administrator systemu informatycznego, pracownicy zatrudnieni w charakterze informatyków jak i osoby świadczące usługi informatyczne na podstawie umów cywilnoprawnych, a także serwisant znajdujących się ww. urządzeń, a osoby postronne w ogóle nie mają dostępu; klucze do pomieszczenia przechowuje Administrator Systemu Informatycznego,
3. pomieszczenie księgowości z kasą pancerną, w którym mogą przebywać wyłącznie pracownicy księgowości, inni użytkownicy danych tylko w towarzystwie pracowników tego działu, a osoby postronne w ogóle nie mają dostępu; klucze do pomieszczenia przechowuje upoważniony pracownik Działu Księgowości,
4. archiwum, w którym mogą przebywać wyłącznie inspektor ochrony danych, kierownik działu administracji, inni użytkownicy danych tylko w towarzystwie kierownika działu administracji, a osoby postronne w ogóle nie mają dostępu; klucze do pomieszczenia przechowuje Kierownik Działu Organizacyjno-Administracyjnego,
5. pomieszczenie zajmowane przez Administratora Systemu Informatycznego, w którym przechowywana jest macierz dyskowa zawierająca kopie robocze systemów informatycznych służących do przetwarzania danych (COMARCH OPTIMA i PŁATNIK); klucze do pomieszczenia przechowuje Administrator Systemu Informatycznego.
6. W pozostałych pomieszczeniach mogą przebywać wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w nich przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie Administratora Danych Osobowych.
7. Niedopuszczalne jest pozostawianie niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu, jeśli nie pozostaje w nim osoba upoważniona.
8. Drzwi do pomieszczeń powinny być wyposażone w zamek mechaniczny.
9. Po zakończeniu dnia pracy, ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zgodnie z obowiązującymi ustaleniami, zabezpieczyć klucze do pomieszczenia.
10. Po godzinach pracy wszystkie dokumenty zawierające informacje istotne z punktu widzenia interesów Biblioteki, w szczególności te zawierające dane osobowe, powinny być przechowywane w zamkniętych szafach lub szufladach, zabezpieczonych przed dostępem do nich osób nieuprawnionych.
11. Należy unikać pozostawionych bez nadzoru dokumentów na biurku. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz innych nośników informacji (płyt CD, DVD, itp.).
12. Pomieszczenie serwerowni oraz miejsce przechowywania kopii danych powinny być wyposażone w odpowiedni sprzęt gaśniczy.
13. W trakcie prac technicznych wykonywanych przez osoby trzecie, przetwarzanie danych osobowych na wydzielonych stanowiskach jest zabronione, a sprzęt komputerowy musi być wyłączony.

§ 19. Ograniczenia dostępu do systemów informatycznych

1. Każdy upoważniony pracownik zobowiązany jest do pracy w systemie informatycznym służącym do przetwarzania danych osobowych na przypisanym mu, indywidualnym koncie.
2. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie pracownik zarejestrowany w tym systemie przez Administratora Systemu Informatycznego na wniosek pracownika odpowiedzialnego w spawach kadr.
3. Pracownik odpowiedzialny w spawach kadr ma obowiązek informowania Inspektora Ochrony Danych, o każdym nowym pracowniku, a także o ustaniu zatrudnienia pracowników zarejestrowanych w tym systemie.
4. Rejestracja, o której mowa w ust. 2, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu informatycznego.
5. Użytkownik systemu informatycznego odpowiedzialny jest za wszystkie czynności wykonywane przy użyciu identyfikatora i hasła użytkownika systemu informatycznego, którymi się posługuje lub posługiwał.

**§ 20. Identyfikator**

1. Identyfikator użytkownika systemu informatycznego:
2. jest przydzielany przez Administratora Systemów Informatycznych na wniosek pracownika odpowiedzialnego w spawach kadr i jest niepowtarzalny,
3. po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielany innej osobie,
4. nie podlega zmianie,
5. jest wpisywany do prowadzonego przez pracownika odpowiedzialnego w sprawach kadr we współpracy z Administratorem Systemów Informatycznych rejestru użytkowników systemu informatycznego wraz z imieniem i nazwiskiem użytkownika systemu informatycznego *(wzór rejestru stanowi załącznik nr 6 do Polityki)*.
6. Użytkownicy systemu informatycznego zobowiązani są do zachowania poufności i nie przekazywania osobom nieuprawnionym udostępnionych im identyfikatorów.

**§ 21. Hasło**

1. Hasło użytkownika systemu informatycznego:
2. jest przydzielane przez Administratora Systemów Informatycznych na wniosek pracownika odpowiedzialnego w spawach kadr, indywidualnie dla każdego z użytkowników systemu informatycznego, a następnie zmieniane przy pierwszym zastosowaniu (zalogowaniu użytkownika do systemu informatycznego) i znane tylko temu użytkownikowi systemu informatycznego,
3. nie jest zapisywane w systemie w postaci jawnej,
4. Użytkownicy systemu informatycznego zobowiązani są do zachowania poufności i nie przekazywania osobom nieuprawnionym używanych przez siebie haseł.
5. Hasła do systemów informatycznych służących do przetwarzania danych zmieniane są nie rzadziej niż raz na miesiąc, a hasła do systemów operacyjnych nie rzadziej niż raz na sześć miesięcy.

§ 22. Praca w systemie

1. Rozpoczęcie pracy w systemie informatycznym odbywa się poprzez:
2. przygotowanie stanowiska pracy,
3. włączenie stacji roboczej,
4. wprowadzenie swojego identyfikatora i hasła użytkownika systemu informatycznego.
5. Zakończenie pracy w systemie informatycznym odbywa się poprzez:
6. zamknięcie aplikacji,
7. odłączenie się od zasobów systemowych,
8. zamknięcie systemu operacyjnego,
9. wyłączenie stacji roboczej.
10. Zawieszenie pracy w systemie informatycznym odbywa się poprzez:
11. aktywację wygaszacza ekranu z hasłem po 15 minutach od momentu bezczynności stacji roboczej,
12. wylogowanie się z systemu informatycznego przez użytkownika systemu informatycznego,
13. zabezpieczenie stacji roboczej po odejściu od stanowiska.

**§ 23. Wyrejestrowanie z sytemu**

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemów Informatycznych na wniosek pracownika odpowiedzialnego w sprawach kadr.
2. Wyrejestrowanie, o którym mowa w ust. l, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
4. zablokowanie konta użytkownika systemu informatycznego do czasu ustalenia przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);
5. usunięcie danych użytkownika systemu informatycznego z bazy użytkowników systemu informatycznego (wyrejestrowanie trwałe).
6. Przyczyną czasowego wyrejestrowania użytkownika systemu informatycznego z systemu informatycznego są w szczególności:
7. nieobecność w pracy trwająca dłużej niż 21 dni kalendarzowych;
8. zawieszenie w pełnieniu obowiązków służbowych;
9. zwolnienie z pełnienia obowiązków służbowych.
10. Przyczyną trwałego wyrejestrowania użytkownika systemu informatycznego z systemu informatycznego są w szczególności:
11. cofnięcie upoważnienia do przetwarzania danych,
12. ustanie zatrudnienia.

§ 24. Kopie robocze - tworzenie

1. Kopie awaryjne tworzy się z następującą częstotliwością:
2. SOWA SQL – codziennie (tworzone są na serwerach dostawcy systemu informatycznego, bez udziału Administratora Systemu Informatycznego, kopie tworzone są automatycznie w czasie nie korzystania z danych na serwerze),
3. kopie pozostałych systemów informatycznych służących do przetwarzania danych osobowych (COMARCH OPTIMA i PŁATNIK) - nie rzadziej niż raz w miesiącu.
4. Kopie robocze systemów informatycznych wymienionych w pkt 2) (COMARCH OPTIMA i PŁATNIK) wykonuje się na dysku sieciowym, a nie rzadziej niż raz na sześć miesięcy zapisuje się je na nośniku DVD. Kopie robocze systemów informatycznych zapisane na nośniku DVD niszczone są po roku od ich wytworzenia.
5. Kopie awaryjne podlegają takiej samej ochronie jak serwery zawierające dane osobowe.

**§ 25. Kopie robocze - przechowywanie**

1. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
2. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
3. Administrator Systemów Informatycznych dokonuje okresowych przeglądów kopii awaryjnych i ocenia ich przydatność do odtworzenia zasobów systemu informatycznego w przypadku jego awarii.
4. Stwierdzenie utraty przez kopię awaryjną waloru przydatności do celu, o którym mowa w ust. 3, upoważnia Administratora Systemów Informatycznych do ich zniszczenia i odnotowania tego faktu.

**§ 26.** **Kopie robocze - usuwanie**

1. Kopie robocze usuwane są po sześciu miesiącach od ich wykonania.
2. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.
3. Niszczenia kopii zapasowych na nośnikach magnetycznych dokonuje Administrator Systemów Informatycznych.

**§ 27. Usuwanie danych**

1. Dane z nośnika należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.
2. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
3. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych osobowych należy wymontować go z komputera i fizycznie zniszczyć
4. Likwidacji dokumentów papierowych zawierających dane osobowe dokonuje się przy użyciu przeznaczonych do tego celu urządzeń (niszczarek).
5. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej możliwości zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały.
6. Trwałego zniszczenia zbędnych nośników informacji i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

**§ 28. Oprogramowanie antywirusowe**

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
2. Oprogramowanie, o którym mowa w ust. l, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemów Informatycznych, nie rzadziej niż raz na trzy miesiące, przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
4. Do obowiązków Administratora Systemów Informatycznych należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.
5. Zabrania się pracownikom blokowania pracy oprogramowania, o którym mowa w ust. 1.
6. W razie niemożliwości usunięcia wirusa, Administrator Systemów Informatycznych ma obowiązek niezwłocznego przedstawienia Inspektorowi Ochrony Danych i Administratorowi Danych Osobowych lub wyznaczonej przez niego osobie, propozycji działań zaradczych. Po usunięciu wirusa Administrator Systemów Informatycznych sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności.

§ 29. Zabezpieczenie sprzętu komputerowego

1. Pracownicy zatrudnieni w charakterze informatyków wskazują użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację urządzeń i systemu informatycznego.
2. Wszystkie urządzenia systemu informatycznego, na których przetwarza się dane osobowe w systemach informatycznych (COMARCH OPTIMA i PŁATNIK) zasilane są za pośrednictwem zasilaczy awaryjnych (UPS).
3. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z szaf dystrybucyjnych zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.
4. Bieżąca konserwacja sprzętu Administratora Danych Osobowych wykorzystywanego do przetwarzania danych osobowych prowadzona jest przez pracowników zatrudnionych w charakterze informatyków lub pod ich nadzorem przez innych upoważnionych.
5. W przypadku konieczności dokonania naprawy przez podmiot zewnętrzny, w siedzibie administratora danych, dokonuje się tego po uprzednim zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych lub po usunięciu tych danych.
6. W szczególnych przypadkach, gdy nie istnieje ryzyko naruszenia ochrony danych osobowych, można dokonać naprawy w warunkach określonych w ust. 5 bez zawarcia umowy o powierzeniu przetwarzania danych i bez usunięcia danych, jednak pod ścisłym nadzorem pracownika działu informatyki dbającego o to, by serwisant nie miał dostępu do danych osobowych administratora danych.
7. Administrator Systemu Informatycznego dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
8. Zużyty lub uszkodzony sprzęt służący do przetwarzania danych osobowych może być zbywany lub utylizowany dopiero po trwałym usunięciu danych, a jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora, po zawarciu umowy powierzenia przetwarzania danych.

**§ 30. Przegląd i konserwacja systemu**

1. Przeglądu i konserwacji systemu, Administrator Systemów Informatycznych dokonuje doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemów Informatycznych dokonuje nie rzadziej niż raz w miesiącu.
3. Przeglądu i sprawdzenia poprawności pracy systemów informatycznych służących do przetwarzania danych osobowych (COMARCH OPTIMA i PŁATNIK), użytkownik systemu informatycznego przy współudziale Administratora Systemów Informatycznych dokonuje nie rzadziej niż raz na miesiąc.

**§ 31. Polityka osobowa**

1. Nabór pracowników na stanowiska związane z przetwarzaniem danych osobowych dokonywany jest z uwzględnieniem kompetencji merytorycznych oraz kwalifikacji moralnych kandydatów. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
2. Dopuszczenie do stanowisk związanych z przetwarzaniem danych osobowych następuje po zrealizowaniu obowiązków wynikających z przepisów prawa oraz niniejszej *Polityki ochrony danych osobowych*, w szczególności po wystawieniu stosownego indywidualnego upoważnienia oraz zapoznaniu osób dopuszczanych do przetwarzania z zasadami dotyczącymi bezpieczeństwa danych osobowych.
3. Ryzyko naruszenia zasad ochrony danych osobowy ze strony osób, które nie zostały upoważnione do przetwarzania danych osobowych (np. personel sprzątający) jest minimalizowane przez odpowiednie przeszkolenie ich (pouczenie) oraz zobowiązywanie do zachowania tajemnicy.

§ 32. Indywidualne wymagania dotyczące użytkowników

Użytkownicy zobowiązani są do zachowania następujących reguł bezpieczeństwa:

1. powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu oraz instalowania nieautoryzowanego oprogramowania, nawet gdyby mogło to usprawnić pracę lub podnieść poziom bezpieczeństwa danych,
2. nietworzenia kopii danych na nośnikach (CD, DVD, FDD, PEN DRIVE, HDD przenośne i inne) bez zezwolenia Administratora Systemu Informatycznego oraz nieużywania nośników wymienionych powyżej do wymiany informacji bez uprzedniego sprawdzenia programem antywirusowym,
3. dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie),
4. niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory),
5. zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,
6. przestrzegania indywidualnych uprawnień i realizacji obowiązków w zakresie przetwarzania danych osobowych, w szczególności właściwego korzystania
z powierzonych sprzętów i udostępnionych zasobów oraz używania wyłącznie własnego identyfikatora i hasła,
7. nieudostępniania stacji roboczej osobom nie zarejestrowanym w systemie,
8. odpowiedniego zabezpieczenia identyfikatora i hasła wymaganego do uwierzytelnienia się w systemie oraz nieudostępniania go innym osobom,
9. w przypadku powzięcia podejrzenia lub stwierdzenia, że z identyfikatorem lub hasłem użytkownika systemu informatycznego mogły zapoznać się osoby trzecie, do niezwłocznego zawiadomienia o tym Inspektora Ochrony Danych oraz Administratora Danych Osobowych, który zwróci się z wnioskiem do Administratora Systemów Informatycznych o nadanie nowego identyfikatora użytkownika systemu informatycznego,
10. zachowania danych osobowych i sposobu ich zabezpieczenia w tajemnicy, w tym także wobec osób najbliższych,
11. ustawiania ekranów komputerowych tak, by osoby nieuprawnione nie widziały treści wyświetlanych na ekranie, w przypadku braku możliwości ustawienia ekranu w taki sposób, by uniemożliwić wgląd, wyłącznik ekranu powinien być łatwo dostępny, aby w każdej chwili wyświetlane informacje wyłączyć z podglądu,
12. ustawienia wygaszacza ekranu włączającego się automatycznie po określonym czasie bezczynności użytkownika,
13. umieszczania na pulpicie komputera jedynie ikon standardowego oprogramowania i aplikacji służbowych oraz skrótów folderów pod warunkiem, że w nazwie nie zawierają informacji o realizowanych projektach lub klientach,
14. niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
15. niepozostawiania bez kontroli włączonych urządzeń zawierających dane osobowe oraz niezabezpieczonych dokumentów (czasowe opuszczania stanowiska pracy jest dopuszczalne dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu urządzenia w inny sposób),
16. zabierania z drukarek drukowanych dokumentów niezwłocznie po wydrukowaniu, przypadku nieudanej próby drukowania, użytkownik powinien skontaktować się z pracownikiem odpowiedzialnym za poprawne funkcjonowanie urządzenia, a następnie samodzielnie lub według instrukcji usunąć informację z pamięci drukarki,
17. niszczenia niepotrzebnych wydruków i kopii dokumentów po ich wykorzystaniu oraz kasowania po wykorzystaniu danych z dysków przenośnych,
18. przekazywania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej,
19. zapisywania plików lub wykonywania kopii roboczych danych, na których się właśnie pracuje, z częstotliwością zapobiegającą ich utracie,
20. dbanie o odpowiednie zabezpieczenie wszelkich dokumentów i wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy (np. w szafie zamykanej na klucz),
21. umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy,
22. zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
23. zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza na portierni, chyba, że niniejsza Polityka stanowi inaczej.

§ 33. Komputery przenośne i praca poza siedzibą administratora

1. Obowiązkiem pracowników użytkujących komputery, w tym komputery przenośne, zawierające dane osobowe jest zachowanie szczególnej ostrożności podczas ich użytkowania, transportu lub przechowywania poza pomieszczeniami tworzącymi obszar, w którym są przetwarzane dane osobowe, a w szczególności stosowanie ochrony kryptograficznej wobec przetwarzanych danych osobowych.
2. Wynoszenie poza obszar przetwarzania danych urządzeń i dokumentów zawierających dane osobowe jest dopuszczalne jedynie za wiedzą i zgodą inspektora ochrony danych lub bezpośredniego przełożonego, gdy konieczność taka została uprzednio uzgodniona z inspektorem ochrony danych oraz wymaga odnotowania tego faktu w ewidencji prowadzonej przez Administratora Systemu Informatycznego.
3. Urządzenia zawierające dane osobowe wynoszone poza obszar przetwarzania danych należy chronić przed uszkodzeniami fizycznymi. Należy też bezwzględnie przestrzegać zaleceń producentów dotyczących ochrony sprzętu. W szczególności należy pamiętać, że urządzenia elektroniczne mogą ulec uszkodzeniu w skutek działanie silnego pola elektromagnetycznego i chronić je przed takim oddziaływaniem.
4. Urządzenia przenośne, nośniki danych oraz dokumenty wynoszone poza obszar przetwarzania danych nie powinny być pozostawiane bez nadzoru. W szczególności zabrania się pozostawiania urządzeń i dokumentów zawierających dane osobowe bez odpowiedniego zabezpieczenia w miejscach publicznych, pokojach hotelowych oraz w samochodach.
5. Wykorzystywanie urządzeń przenośnych, nośników danych oraz dokumentów zawierających dane osobowe w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko utraty, zniszczenia lub zapoznania się z danymi przez osoby nieupoważnione. Za miejsca szczególnego ryzyka należy uznać restauracje oraz środki komunikacji publicznej.
6. Niedozwolone jest udostępnianie urządzeń przenośnych i nośników danych należących do administratora danych osobom nieupoważnionym, w tym domownikom i osobom bliskim użytkownika. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych lub chroniącym dostęp do nośników danych.
7. Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa termin i zasady zwrotu sprzętu.

===================================================================

§ 34. Zasady ochrony danych osobowych

1. **Zasada legalności przetwarzania.** Należy zapewnić, by dane osobowe były przetwarzane wyłącznie po spełnieniu jednego z warunków dopuszczalności przetwarzania określonych w art. 6 ust. 1 RODO, a w przypadku szczególnych kategorii danych (tzw. danych wrażliwych) art. 9 i art. 10 RODO.
2. **Zasada rzetelności przetwarzania.** Przetwarzanie rzetelne należy rozumieć jako przetwarzanie uczciwie w stosunku do osoby, których dane dotyczą. Podejmując dowolne czynności przetwarzania należy brać pod uwagę (respektować) prawa i interesy podmiotów danych. Należy wziąć pod uwagę, że przetwarzanie może być dokuczliwe dla podmiotu danych i spróbować zminimalizować te uciążliwości. Nie można też próbować oszukiwać, ani wykorzystywać braku wiedzy lub trudnej sytuacji podmiotu danych.
3. **Zasada przejrzystości przetwarzania.** Należy zapewnić przejrzystą informację podmiotom danych o dotyczącym ich przetwarzaniu. Powinny być stworzone ścieżki komunikacji umożliwiające zainteresowanym skorzystanie z przyznanych im praw.
4. **Zasada ograniczoności celu.** Dane wolno zbierać jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie wolno ich przetwarzać po zebraniu w sposób niezgodny z tymi celami. Do celu należy dostosować nie tylko ilość zbieranych danych, ale też zakres ich przetwarzania oraz okres, przez który są przechowywane.
5. **Minimalizacja danych.** Dane powinny być adekwatne do celu, czyli ograniczone do niezbędnego minimum. Metodą urzeczywistnienia tej zasady może być m.in. pseudonimizacja. Gdy cel przetwarzania tego nie wymaga to w ogóle nie należy dokonywać identyfikacji osobowej.
6. **Prawidłowość danych.** Dane powinny być prawdziwe (zgodne z prawdą) i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
7. **Ograniczenie przechowywania.** Dane wolno przechowywać w formie umożliwiającej identyfikację osoby, której one dotyczą, jedynie przez okres niezbędny dla realizacji celów, w których dane te są przetwarzane.

§ 35. Realizacja obowiązków informacyjnych i zapewnienie przejrzystej komunikacji

1. Informacje przekazywane podmiotom danych należy formułować w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
2. Należy uprawdopodobnić, że informacje są przekazywane osobie, której dane dotyczą. W razie wątpliwości należy zażądać dodatkowych informacji w celu zweryfikowania tożsamości, osoby, która się kontaktuje w celu uzyskania informacji.
3. Przekazując informacje podmiotowi danych należy zadbać o to, by informacja ta obejmowała wyłącznie dane go dotyczące. Należy dołożyć starań, by informacja przekazywana jednej osobie nie zdradzała informacji o innych.
4. Zbierając informacje bezpośrednio od osoby, której dotyczą należy jednocześnie przekazać tej osobie informacje wskazane w art. 13 ust. 1 i 2 RODO. Obowiązek ten należy zrealizować w trakcie pozyskiwania informacji.
5. Gdy dane są zbierane z innego źródła niż od osoby, której dotyczą to należy spełnić obowiązek informacyjny w zakresie art. 14 ust. 1 i 2 RODO. Należy to zrobić
w rozsądnym terminie (do miesiąca) od zebrania informacji, nie później jednak niż przy pierwszej komunikacji z podmiotem danych lub pierwszym udostępnieniem danych.
6. Stosowną informację w zakresie art. 13 ust. 1 i 2 lub art. 14 ust. 1 i 2 RODO należy podmiotowi danych przekazać także w przypadku zmiany celu przetwarzania dokonanym po zebraniu danych, chyba, że został już o tym uprzedzony.
7. Należy zapewnić ścieżki komunikacji umożliwiające osobom, których dane dotyczą kontakt w celu realizacji przyznanych im praw.

§ 36. Realizacja żądań osób, których dane dotyczą

1. Jeżeli zainteresowany skorzysta z prawa dostępu do danych (zażąda informacji na temat dotyczącego go przetwarzania) to udziela się mu jej zgodnie z art. 12 ust. 1 i 2 RODO. Jeśli podmiot danych tego zażąda, a jest to możliwe, przekazuje się mu także kopię dotyczących go danych. Informacji na żądanie udziela się zasadniczo w terminie miesiąc, chyba, że sprawa jest skomplikowana. Wtedy przedłużenie terminu następuje zgodni z art. 12 ust. 3 RODO.
2. Jeżeli zainteresowany skorzysta z prawa do sprostowania to na jego żądanie dokonuje się sprostowania nieprawidłowych danych. Prawo to obejmuje też uzupełnienie niekompletnych danych, przy czym kompletność ocenia się z uwzględnieniem celów przetwarzania. O ile to możliwe to o dokonanym sprostowaniu informuje się odbiorców, którym dane zostały przekazane.
3. Jeżeli zainteresowany skorzysta z prawa do usunięcia danych (bycia zapomnianym) to na jego żądanie usuwa się dotyczące go dane, chyba że spełnione są wymogi ich dalszego przetwarzania z art. 17 ust. 3 RODO. O ile to możliwe to o dokonanym usunięciu informuje się odbiorców, którym dane zostały przekazane. Gdy dane zostały upublicznione należy podjąć starania w celu usunięcia wszelkich łączy do tych danych, ich kopii lub replikacji stworzonych przez innych administratorów.
4. Jeżeli zainteresowany skorzysta z prawa do ograniczenia przetwarzania to na jego żądanie należy ograniczyć przetwarzanie do wskazanych czynności, chyba, że zachodzą przesłanki ich dalszego przetwarzania, w szczególności te wymienione w art. 18 ust. 2 RODO. O ile to możliwe to o dokonanym ograniczeniu informuje się odbiorców, którym dane zostały przekazane.
5. Jeżeli zainteresowany skorzysta z prawa do przeniesienia danych to dostarcza mu się dotyczących go danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Prawo to przysługuje, gdy dane mają postać zapisu elektronicznego i są przetwarzane na podstawie warunku zgody lub realizacji umowy. Na żądanie zainteresowanego dane dostarcza się bezpośrednio wskazanemu przez niego podmiotowi.
6. Jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych osobowych, w tym profilowania, powołując się na swoją szczególną sytuację, to należy zaprzestać dalszego przetwarzania dotyczących go danych, chyba, że spełnione są przesłanki dalszego przetwarzania określone w art. 21 ust. 1 RODO.
7. Jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych w celach marketingowych, w tym profilowania, to nie można nie uwzględnić sprzeciwu.

§ 37. Zgoda na przetwarzanie danych osobowych

1. Jeżeli zgodnie z art. 6 ust. 1 lub 9 ust. 1 RODO podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą to przyzwolenie na przetwarzanie danych powinno być dobrowolne, konkretne, świadome i jednoznaczne. Musi spełniać też wymogi rozliczalności i transparentności.
2. Zapewnia się prawo do wycofania zgody.
3. Nie jest dopuszczalne uzależnienie wykonania usługi niezwiązanej bezpośrednio ze zgodą od jej udzielenia.
4. W przypadku usług społeczeństwa informacyjnego oferowanych dziecku podejmuje się wszelkie niezbędne działania by uzyskać aprobatę opiekuna.

§ 38. Udostępnianie danych osobowych

1. Jeśli zgodnie z przepisami prawa administrator danych jest zobowiązany do przekazywana danych osobowych wskazanym podmiotom (np. Urzędowi Skarbowemu lub ZUS) to upoważnieni pracownicy administratora danych realizują ten wymóg zgodnie z zakresem swoich obowiązków służbowych stosując się ściśle do wskazanych przepisów.
2. Jeśli do administratora danych wystąpi z wnioskiem o udzielenie informacji osobowej podmiot, który twierdzi, że jest uprawniony do uzyskania takiej informacji na podstawie przepisów prawa udostępnienie informacji może nastąpić jedynie po:
3. zweryfikowaniu podstawy prawnej udostępnienia,
4. zweryfikowaniu czy składający wniosek jest podmiotem za który się podaje,
5. odnotowaniu udostępnienia w ewidencji udostępnień danych osobowych.
6. Ewidencję udostępnień danych osobowych prowadzi inspektor ochrony danych osobowych.
7. W przypadku, gdy z wnioskiem o którym mowa ust. 2 wystąpi uprawniony funkcjonariusz, w szczególności policji, i wnioskujący stwierdzi, że istnieje konieczność niezwłocznego działania udostępnienie informacji może nastąpić po:
8. wylegitymowaniu funkcjonariusza,
9. na podstawie pisemnego oświadczenia funkcjonariusza lub za pisemnym pokwitowaniem przez niego uzyskania dokumentów.
10. Jeśli złożenie oświadczenia lub pokwitowanie uzyskania danych przez funkcjonariusza nie są możliwe ze względu na okoliczności udostępniania, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

§ 39. Przekazywanie danych do państw trzecich lub organizacji międzynarodowym

1. Przekazywanie danych osobowych do państw trzecich jest zasadniczo zabronione, chyba, że decyzję taką podejmie administrator danych, ze względu na szczególne okoliczności.
2. W przypadku określonym w ust. 1 przekazanie jest dokonywane wyłącznie zgodnie z wymogami określonymi w art. 44-50 RODO. Administrator danych dokłada staranności, by zapewnić stopień ochrony osób fizycznych zagwarantowany w RODO.

§ 40. Współpraca z podmiotami przetwarzającymi

1. Jeśli wymagają tego okoliczności administrator danych może podjąć decyzje
o powierzeniu przetwarzania danych osobowych podmiotowi przetwarzającemu.
2. Wybierając podmiot przetwarzający administrator danych dokłada staranności, by podmiot ten zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO.
3. Powierzenie danych osobowych podmiotowi przetwarzającemu następuje na podstawie pisemnej umowy określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora danych i podmiotu przetwarzającego.
4. Umowa o której mowa w ust. 3 zawiera, jeśli to właściwe, w szczególności:
	1. zobowiązanie przetwarzającego do tego, że przetwarzanie danych osobowych będzie się odbywało wyłącznie na udokumentowane polecenie administratora danych,
	2. deklarację przetwarzającego, że osoby upoważnione przez niego do przetwarzania danych osobowych zobowiązały się lub zobowiążą do zachowania w tajemnicy dane osobowe oraz sposób ich zabezpieczenia,
	3. deklarację przetwarzającego, że wdrożył lub wdroży odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa zgodnie z art. 32 RODO,
	4. deklarację przetwarzającego wskazującą, że jeśli korzysta lub będzie korzystać z usług innego podmiotu przetwarzającego, to wypełnia lub wypełni warunki określone w art. 28 ust. 2 i 4 RODO,
	5. zobowiązanie przetwarzającego do pomocy administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w pkt. 1-7,
	6. zobowiązanie przetwarzającego do pomocy administratorowi danych
	w realizacji obowiązków określonych w częściach VIII i IX niniejszej Polityki,
	7. zobowiązanie przetwarzającego do usunięcia lub zwrotu wszelkich danych osobowych administratora oraz wszelkich ich istniejących kopii po zakończeniu świadczenia usług, jeśli administrator danych wystąpi z takim żądaniem.
5. Umowy z podmiotami przetwarzającymi są przekazywane inspektorowi ochrony danych w celu włączenia ich do dokumentacji ochrony danych osobowych.

§ 41. Współadministrowanie

1. Jeśli wymagają tego okoliczności administrator danych może podjąć decyzje
o wspólnym ustaleniu celów i sposobów przetwarzania danych osobowych z innym administratorem (tzw. współadministrowanie).
2. Uzgodnienie wskazane w ust. 1 jest zawierane w formie umowy pisemnej.
3. Umowa o której mowa w ust. 2 w przejrzysty sposób:
4. określa odpowiednie zakresy odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności obowiązków informacyjnych oraz innych obowiązków względem osób, których dane dotyczą,
5. wskazuje jak osoby, których dane dotyczą mogą kontaktować się w celu uzyskania informacji i realizacji przysługujących im praw.
6. Umowa o której mowa w ust. 1 w zakresie w jakim dotyczy osób, których dane mają być przetwarzane jest udostępniana tym osobom na ich żądanie.

§ 42. Nadzór nad przestrzeganiem ochrony danych osobowych

1. W celu zapewnienia ochrony wolności i praw osób, których dane dotyczą,
a zwłaszcza bezpieczeństwa dotyczących ich danych inspektor ochrony danych osobowych:
2. dokonuje inwentaryzacji zasobów danych osobowych i dba o aktualność ich opisu,
3. przeprowadza ocenę ryzyka naruszenia ochrony danych osobowych,
4. jeśli to wymagane prowadzi rejestr czynności przetwarzania,
5. jeśli to wymagane przeprowadza ocenę skutków dla ochrony danych,
6. jeśli to wymagane prowadzi uprzednie konsultacje z organem nadzorczym,
7. czuwa nad aktualnością dokumentacji z zakresu ochrony danych osobowych,
8. czuwa nad przestrzeganiem zasad określonych w dokumentacji ochrony danych osobowych,
9. czuwa nad zgodnością przetwarzania danych osobowych z przepisami
o ochronie danych osobowych,
10. prowadzi postępowanie wyjaśniające w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych.
11. W celu realizacji zadań określonych w ust. 2 lit. f) - h) inspektor ochrony danych przeprowadza okresowe audyty wewnętrzne (tzw. sprawdzenia planowe). Realizując zadanie określone w ust. 2 lit. i) inspektor ochrony danych przeprowadza audyt wewnętrzny nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne).
12. Inspektor ochrony danych zapewnia (nadzoruje) realizację obowiązku zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie tych danych, w szczególności decyduje o terminach i sposobach przeprowadzenia szkoleń w tym zakresie.

§ 43. Inwentaryzacja i opis zasobów

1. Inspektor ochrony danych dba o to, by przetwarzanie danych osobowych w Bibliotece odbywało się wyłącznie za wiedzą, zgodą i pod nadzorem upoważnionych.
2. W celu realizacji zadania określonego w ust. 1. inspektor ochrony danych opisuje zasoby danych osobowych oraz sposób ich przetwarzania i zabezpieczenia*.*
3. Inspektor ochrony danych dba o aktualność opisu zasobów. Ocena aktualności opisu zasobów stanowi element okresowego przeglądu dokumentacji.

§ 44. Rejestr czynności przetwarzania

1. Biblioteka prowadzi rejestr czynności przetwarzania tak, by był on zgodny z wymogami art. 30 RODO. Przeprowadzając okresowy przegląd dokumentacji Inspektor Ochrony Danych dokonuje oceny spełnienia powyższego wymogu.
2. Inspektor Ochrony Danych przekazuje rejestr czynności przetwarzania organowi nadzorczemu na jego żądanie.

§ 45. Ocena ryzyka

1. Celem oceny ryzyka jest ustalenie czy stopień bezpieczeństwa danych jest odpowiedni oraz czy nie zachodzi niebezpieczeństwo naruszenia praw i wolności osób fizycznych.
2. Administrator danych zleca inspektorowi ochrony danych przeprowadzenie oceny ryzyka, gdy:
3. są planowane lub podejmowane nowe czynności z wykorzystaniem danych osobowych,
4. dokonywane są zmiany sposobu działania Biblioteki, w szczególności zmiany w zakresie wykorzystywanej technologii i organizacji pracy, gdy może to mieć wpływ na przetwarzanie danych osobowych.
5. Wyniki oceny ryzyka Inspektor Ochrony Danych przedstawia niezwłocznie administratorowi danych. Jeśli na skutek przeprowadzonej oceny inspektor ochrony danych ustali, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to administrator danych rezygnuje z planowanych działań, albo podejmuje czynności wskazane w ust. 4.
6. Jeśli administrator danych chce kontynuować planowane działania mimo, że z oceny ryzyka wynika, że z dużym prawdopodobieństwem mogą one powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to:
	1. zleca właściwym podmiotom, w tym inspektorowi ochrony danych, opracowanie i zastosowanie środków zaradczych, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie postanowień RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy,
	2. zleca inspektorowi ochrony danych przeprowadzenie oceny skutków przetwarzania dla ochrony danych osobowych zgodnie z ust. 5.
	3. oceny skutków przetwarzania dla ochrony danych wskazanej w ust.4 nie trzeba przeprowadzać, gdy przetwarzanie jest obowiązkiem wynikającym
	z przepisu prawa lub jest niezbędne do wykonania zadania realizowanego
	w interesie publicznym lub w ramach sprawowania władzy publicznej.
7. Ocenę ryzyka inspektor ochrony danych przeprowadza także w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych zgodnie z częścią VIII niniejszej Polityki.

§ 46. Ocena skutków przetwarzania dla ochrony danych

1. Jeżeli administrator danych osobowych zlecił pełnomocnikowi bezpieczeństwa informacji przeprowadzenie oceny skutków przetwarzania dla ochrony danych zgodnie z § 4 ust. 4. lit. b), to inspektor ochrony danych przystępuje niezwłocznie do opracowania takiej oceny.
2. Ocena skutków o której mowa w ust. 1. obejmuje:
	1. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora,
	2. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne
	w stosunku do celów,
	3. wskazanie środków zaplanowanych w celu zaradzenia ryzyku, ze szczególnym wyróżnieniem tych opracowanych i wdrożonych w ramach działań podjętych na zlecenie wskazane w § 4 ust. 4. lit. a),
	4. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, po zastosowaniu środków wskazanych w ust. 2. lit. c).
3. Wyniki oceny skutków inspektor ochrony danych przedstawia niezwłocznie administratorowi danych. Jeśli ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby nadal wysokie ryzyko naruszenia wolności lub praw osób, których dane dotyczą, a zastosowane środki wskazane w § 5 ust. 2. lit. c) nie pozwalają na jego zminimalizowanie, to administrator danych rezygnuje się z podejmowania planowanych działań, albo przedstawia sprawę organowi nadzorczemu w trybie uprzednich konsultacji zgodnie z § 6.

§ 47. Uprzednie konsultacje z organem nadzorczym

1. Jeśli w sytuacji określonej w § 5 ust. 3. administrator danych podejmie decyzję o przeprowadzeniu uprzednich konsultacji z organem nadzorczym nakazuje inspektorowi ochrony danych przygotowanie odpowiedniej dokumentacji dla tego organu.
2. Informacja przygotowana dla organu nadzorczego obejmuje:
	1. wskazanie celów i sposobów zamierzonego przetwarzania,
	2. wskazanie środków i zabezpieczeń mających chronić prawa i wolności osób, których dane dotyczą,
	3. kopię oceny skutków dla ochrony danych, o której mowa w § 5,
	4. dane kontaktowe inspektora ochrony danych.

3. Administrator danych stosuje się do zaleceń wydanych przez organ nadzorczy
w ramach konsultacji. Jeśli organ nadzorczy wystąpi z żądaniem udzielenia dodatkowych informacji to administrator zleca ich przygotowanie pełnomocnikowi bezpieczeństwa informacji.

§ 48. Audyty wewnętrzne

1. W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych inspektor ochrony danych przeprowadza następujące audyty wewnętrzne:
2. sprawdzenie prawidłowości i aktualności dokumentacji z zakresu ochrony danych osobowych,
3. sprawdzenie przestrzegania zasad i procedur określonych w dokumentacji ochrony danych osobowych,
4. sprawdzanie zgodności przetwarzania danych osobowych z przepisami
o ochronie danych osobowych.
5. Audyty wewnętrzne wskazane w ust. 1. są przeprowadzane okresowo zgodnie z planem sprawdzeń przygotowywanym przez inspektora ochrony danych (sprawdzenia planowe). Plan sprawdzeń obejmuje maksimum 1 rok. Jest on przekazywany administratorowi danych do wiadomości w terminie minimum 2 tygodni przed rozpoczęciem okresu, który plan obejmuje. Jeśli sprawdzenie planowe obejmuje kontrolę w konkretnej jednostce lub dziale to kierownik tej jednostki jest zawiadamiany o sprawdzeniu nie później niż na 7 dni przed rozpoczęciem sprawdzenia.
6. W sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, inspektor ochrony danych przeprowadza audyt nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne). W przypadku sprawdzeń doraźnych terminy określone w ust. 2. nie obowiązują.
7. Pełnomocnik bezpieczeństwa informacji przygotowuje i gromadzi dokumentację przeprowadzonych audytów.
8. Obowiązki określone w ust. 1. – 4. inspektor ochrony danych realizuje we współpracy z administratorem systemu oraz kierownikiem działu administracji posługując się w razie potrzeby pracownikami zatrudnionymi w charakterze informatyków.

§ 49. Zapewnienie aktualności dokumentacji z zakresu ochrony danych osobowych

1. Inspektor ochrony danych dokłada starań by dokumentacja ochrony danych osobowych była aktualna. W tym celu na bieżąco śledzi zmiany stanu prawnego oraz zapoznaje się z treścią wytycznych i wskazówek wydawanych przez organ nadzorczy w tym zakresie.
2. Niezależnie od działań wskazanych w ust. 1 inspektor ochrony danych nie rzadziej niż raz do roku dokonuje przeglądu dokumentacji pod kątem sprawdzenia jej aktualności i zgodności z przepisami.

§ 50. Zapewnienie przestrzegania zasad określonych w dokumentacji ochrony danych osobowych

1. Inspektor Ochrony Danych prowadzi bieżący nadzór nad działalnością Biblioteki związaną z przetwarzaniem danych osobowych. Realizując powyższe zadanie inspektor ochrony danych m.in. na bieżąco ocenia zagrożenia, sprawdza kluczowe punkty bezpieczeństwa, formułuje zalecenia i wskazówki, odpowiada na pytania i udziela porad.
2. Niezależnie od działań wskazanych w ust. 1. Inspektor Ochrony Danych nie rzadziej niż raz do roku przeprowadza audyt przestrzegania zasad i procedur ochrony danych osobowych w Bibliotece.
3. W ramach audytu określonego w ust. 2. dokonuje się w szczególności analizy zagrożeń określonych w części IV niniejszej Polityki oraz sprawdza realizację wskazań i obowiązków określonych w części V niniejszej Polityki.

§ 51. Zapewnienie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

1. Inspektor Ochrony Danych: na bieżąco śledzi zmiany prawne i zapoznaje się ze wskazówkami organu nadzorczego wydanymi w zakresie ich wdrożenia, informuje administratora danych o planowanych zmianach prawnych i w porozumieniu z nim oraz, gdy to właściwe, z udziałem administratora systemu, przygotowuje projekty dostosowujące działania, zasady i procedury wewnętrzne do nowych wymogów.
2. Niezależnie od działań wskazanych w ust. 1. inspektor ochrony danych nie rzadziej niż raz do roku przeprowadza audyt zgodności przetwarzania danych osobowych z przepisami.
3. W ramach audytu określonego w ust. 1 dokonuje się w szczególności oceny realizacji wymogów wskazanych w części VI niniejszej Polityki.

§ 52. Postępowanie w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych

1. Przepisami niniejszej Polityki określa się zasady postępowania w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego.
2. Każdy kto stwierdził inne niż określone w ust. 1. naruszenie ochrony danych osobowych lub podejrzewa takie naruszenie powinien niezwłocznie poinformować o tym inspektora ochrony danych. Jako inne niż określone w ust. 1 naruszenie rozumie się w szczególności brak realizacji lub niewłaściwą realizację wymogów określonych w części VI niniejszej Polityki.
3. Inspektor Ochrony Danych po otrzymaniu zawiadomienia, o którym mowa w ust. 2. przeprowadza niezwłocznie postępowanie wyjaśniające w celu ustalenia czy naruszenie ochrony danych osobowych miało miejsce (tzw. sprawdzenie doraźne).
4. Sprawdzenie doraźne może zostać wszczęte przez inspektora ochrony danych także z własnej inicjatywy, gdy w inny sposób niż w skutek zawiadomienia poweźmie informację o naruszeniu lub możliwym naruszeniu ochrony danych osobowych.
5. W przypadku stwierdzenia naruszenia ochrony danych osobowych w trybie określonym w ustępach poprzedzających pełnomocnik bezpieczeństwa informacji:
	1. w porozumieniu z odpowiednim kierownikiem działu podejmuje niezwłoczne, możliwe do wprowadzenia na bieżąco, działania zapobiegające dalszemu naruszaniu ochrony danych osobowych,
	2. w porozumieniu z odpowiednim kierownikiem działu stosuje niezwłoczne, możliwe do wprowadzenia na bieżąco, środki eliminujące lub zmniejszające ryzyko naruszenia praw lub wolności osoby, której dane dotyczą,
	3. sporządza raport naruszenia ochrony danych osobowych, a następnie niezwłocznie przekazuje jego kopię administratorowi danych.
6. Raport o którym mowa w ust. 5. lit. c) zawiera w szczególności:
	1. opis okoliczności naruszenia ochrony danych osobowych,
	2. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
	3. opis możliwych konsekwencji naruszenia ochrony danych osobowych,
	4. ocenę czy jest prawdopodobne, że naruszenie skutkowało ryzykiem lub wysokim ryzykiem naruszenia wolności lub praw osób fizycznych,
	5. wskazanie zastosowanych lub proponowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które zmierzają do zminimalizowania ewentualnych negatywnych skutków naruszenia.
7. Administrator danych osobowych po zapoznaniu się z raportem, o którym mowa
w ust. 6. podejmuje decyzje o dalszym trybie postępowania, a w szczególności:
	1. jeśli to właściwe, zarządza podjęcie czynności zmierzających do usunięcia naruszenia i jego skutków oraz zapobieżeniu naruszeniom ochrony danych osobowych na przyszłość,
	2. jeśli to możliwe, zarządza zastosowanie środków eliminujących lub zmniejszających prawdopodobieństwo ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
	3. jeśli jest to właściwe zawiadamia o naruszeniu właściwe organy, w tym zgłasza naruszenie organowi nadzorczemu oraz informuje o naruszeniu osoby, których naruszenie dotyczy. Do zgłasza naruszeni organowi nadzorczemu zgodnie z art. 33 ust. 1 RODO oraz zawiadamia o naruszeniu osób, których dane dotyczą zgodnie z art. 34 ust. 1 RODO stosuje się postanowienia pkt. 2 i 3 niniejszej części.

§ 53. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu i zawiadomienie osoby, której dane dotyczą.

1. Jeśli administrator danych ustali, że jest prawdopodobne, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w § 1 skutkowało ryzykiem naruszenia wolności lub praw osób fizycznych nakazuje inspektorowi ochrony danych przygotowanie projektu zgłoszenia naruszenia organowi nadzorczemu,
2. Zgłoszenie naruszenia wskazane w ust. 1. zawiera, w szczególności:
	1. informacje zawarte w raporcie, zgodnie z § 1 ust. 6,
	2. wskazanie imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych, jako osoby właściwej do kontaktu w sprawie.
3. Zgłoszenie naruszenia ochrony danych osobowych, o którym mowa w ustępach poprzedzających administrator danych zatwierdza i przekazuje organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
4. Jeżeli dotrzymanie terminu wskazanego w ust. 3. jest niemożliwe administrator danych do zgłoszenia dołącza wyjaśnienie przyczyn opóźnienia. Jeżeli (i w zakresie, w jakim) informacji nie da się udzielić od razu, administrator danych udziela tych informacji sukcesywnie, bez zbędnej zwłoki.

**§ 54. Zawiadomienie osoby, której dane dotyczą.**

1. Jeśli administrator danych ustali, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w § 1 może powodować wysokie ryzyko naruszenia wolności lub praw osób fizycznych i nie da się zastosować środków eliminujących to wysokie ryzyko, nakazuje inspektorowi ochrony danych przygotowanie projektu zawiadomienia o naruszeniu dla wszystkich osób, których danych naruszenie dotyczy.
2. Zawiadomienie o którym mowa w ust. 1 powinno być napisane jasnym i prostym językiem oraz zawierać, w szczególności:
	1. opis charakteru naruszenia,
	2. opis możliwych konsekwencji naruszenia,
	3. wskazanie zastosowanych lub planowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które mogą zminimalizować ewentualne negatywne skutki naruszenia,
	4. wskazanie imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych, jako osoby właściwej do kontaktu w sprawie.
3. Zawiadomienie o naruszeniu ochrony danych osobowych, o którym mowa w ustępach poprzedzających administrator danych zatwierdza i przekazuje niezwłocznie wszystkim osobom, których danych naruszenie dotyczy.
4. Jeżeli administrator danych oceni, że realizacja ww. wymogów wymagałaby niewspółmiernie dużego wysiłku, w szczególności niewspółmiernie dużego wysiłku wymagałoby nawiązanie bezpośredniego, indywidualnego kontaktu z osobami, których danych naruszenie dotyczy, może podjąć decyzje o przekazaniu informacji zainteresowanym poprzez wydanie publicznego komunikatu lub o zastosowaniu innego podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§ 55. Dokumentacja naruszenia ochrony danych osobowych.

1. Inspektor Ochrony Danych prowadzi dokumentację naruszenia danych osobowych.
2. W skład dokumentacji o której mowa w ust. 1. wchodzą:
	1. kopia raportu, o którym mowa w § 1. ust. 6.,
	2. kopia zgłoszenia, o którym mowa w § 2.,
	3. kopie zawiadomień, o których mowa w § 3.,
	4. wszelkie inne dokumenty, w tym notatki służbowe, pliki, zdjęcia i inne dowody zebrane w trakcie przeprowadzania czynności wyjaśniających pozwalające ustalić okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
3. Dokumentacja naruszenia ochrony danych osobowych pozostaje do wglądu organu nadzorczego.

**§ 56. Przepisy przejściowe**

1. Wszyscy pracownicy przetwarzający dane osobowe w Bibliotece zobowiązani są niezwłocznie dostosować swoje działania do wymogów niniejszej Polityki.
2. Inspektor Ochrony Danych niezwłocznie podejmie działania zmierzające do dostosowania lub opracowania brakujących dokumentów, ewidencji, wzorów i formularzy, o których mowa w niniejszej Polityce.

**§ 57. Postanowienia końcowe**

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się i stosować do zasad i procedur określonych w niniejszej Polityce.
2. Naruszenie zasad i procedur określonych w niniejszej Polityce może być stanowić podstawę odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa, a w szczególności może być uznane za ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy albo nienależyte wykonanie umowy w rozumieniu Kodeksu Cywilnego.
3. **Polityka Ochrony Danych wchodzi w życie z dniem 1 stycznia 2019r.**

**Załącznik nr 9a do Polityki Ochrony Danych**

**Procedura zgłoszeń serwisowych**

1. Zgłoszenia serwisowe, gwarancyjne są przyjmowane w dni robocze, w godzinach od 7:00 do 15:00.
2. Pracownik / kierownika działu / filii zgłasza osobie odpowiedzialnej za obsługę informatyczną jednostki fakt wystąpienia usterki / wady niezwłocznie, nie później niż w terminie 1 dni roboczych od dnia jej wystąpienia.
3. Pracownik od chwili wystąpienia usterki / wady wstrzymuje się z dalszą eksploatacją Urządzenia.
4. Zgłoszenia należy dokonać w formie telefonicznej oraz poprzez wiadomość e-mail na adres informatyk@biblioteka.wloclawek.pl.
5. Zgłoszenia są przyjmowane przez bibliotekarza systemowego lub osobę go zastępującą.
6. Jeśli zgłoszenie dotyczy niepoprawności w działaniu usług zewnętrznych następuje kontakt z ich dostawcami.
7. Bibliotekarz systemowy lub osobę go zastępującą po otrzymaniu poprawnie dokonanego zgłoszenia przez pracownika, dokonuje weryfikacji zgłoszenia pod względem formalnym i poprawności podanych informacji.
8. Reakcja polega na wysłaniu do pracownika / kierownika działu / filii informacji zwrotnej na adres email podany w zgłoszeniu lub/i oddzwonienie na numer podany w zgłoszeniu. W udzielonej odpowiedzi podane są informacje instruktażowe umożliwiające samodzielne usunięcie usterki/wady przez pracownika (zgodnie z instrukcją obsługi urządzenia którą Klient otrzymał odbierając urządzenie zgodnie z protokołem odbioru) lub informacja nt. ewentualnego przyjścia / przyjazdu do Pracownika na miejsce celem weryfikacji usterki/wady zgłaszanej na miejscu i podjęcia działań naprawczych.
9. Po przesłaniu mailem do pracownika / kierownika działu / filii informacji zwrotnej zgodnie z pkt. 7. Pracownik / kierownik działu / filii udziela odpowiedzi tą samą drogą komunikacji (email) potwierdzając tym samym: - podjęcie samodzielnych działań lub/i żądanie przyjazdu Bibliotekarza Systemowego lub osobę go zastępującą na miejsce
10. Po otrzymaniu od Pracownika potwierdzenia emailem określającego sposób załatwienia zgłoszenia jak w pkt. 7 wystawia zlecenie wyjazdu serwisowego i w uzgodnionym terminie bibliotekarz systemowy lub osobę go zastępującą jest u pracownika / kierownik działu / filii.
11. Po odbyciu serwisu, raport serwisowy jest ewidencjonowany w teczce zgłoszeń serwisowych.

**Załącznik nr 9b do Polityki Ochrony Danych**

**Procedury** **zabezpieczenia jednostek komputerowych, korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci teleinformatycznej w Bibliotece**

**oraz monitoringu korzystania z komputerów służbowych**

**§ 1. Postanowienia ogólne**

1. Regulamin ustala zasady:
2. zabezpieczenia jednostek komputerowych,
3. korzystania z komputerów służbowych,
4. monitorowania komputerów służbowych,
5. nadzoru nad bezpieczeństwem Systemu Teleinformatycznego w Miejskiej Bibliotece Publicznej im. Zdzisława Arentowicza we Włocławku,
6. nadzoru nad ochroną danych osobowych w bibliotece.
7. Celem wdrożenia Regulaminu jest wprowadzenie zasad korzystania z sieci teleinformatycznej(internetu) przez Pracowników biblioteki, a w szczególności:
8. poprawa jakości i zgodności z procedurami obowiązującymi w bibliotece wykonywania pracy,
9. zabezpieczenie uzasadnionych interesów pracodawcy,
10. ochrona bezpieczeństwa,
11. zabezpieczenie danych oraz mienia pracodawcy.

**§ 2. Zasady zabezpieczenia jednostek komputerowych**

1. Jednostki komputerowe posiadają zabezpieczenie w postaci oprogramowania zapewniające ochronę przed złośliwym oprogramowaniem (ransomware, phishing, ataki 0-day, wirusy, spyware itp.).
2. Jednostki komputerowe posiadają zablokowane strony internetowe z kategorii: broń, hakerstwo, hazard, hosting (udostępnianie i przesyłanie plików), narkotyki, okultyzm, oszustwa, piractwo komputerowe, pornografia, randki online, religia (sekty), samobójstwo, sieciowe serwery proxy, treści dla dorosłych, zdjęcia online.
3. Oprogramowanie posiada możliwość blokowania stron internetowych, które są dozwolone po wykryciu na nich niedozwolony kod lub oprogramowanie.
4. Zablokowane zostały następujące elementy wyposażenia komputera: napędy CD-ROM (możliwość nagrywania danych), stacje dyskietek, przenośne urządzenia Windows, porty Com / LPT, pamięć wewnętrzna oraz zewnętrzna.
5. Skanowanie wszystkich jednostek komputerowych pod kątem bezpieczeństwa wykonywane jest co 1. m-c.

**§ 3.** **Zasady korzystania z oprogramowania**

1. Zobowiązuje się pracowników do korzystania wyłącznie z legalnego oprogramowania.
2. Instalacje oprogramowania na stanowiskach komputerowych mogą być dokonywane z nośników znajdujących się w zasobach biblioteki lub z udostępnionego przez dostawcę oprogramowania serwera. Ich instalacja może być dokonywana wyłącznie przez osobę prowadzącą obsługę informatyczną w instytucji.
3. Pracownik nie może dokonywać żadnych instalacji oprogramowania.
4. Oprogramowanie w wersjach testowych lub w jakikolwiek inny sposób ograniczone umowami licencyjnymi może być użytkowane wyłącznie zgodnie z jego przeznaczeniem i w czasie określonym w umowie licencyjnej.
5. Zabrania się pobierania i kopiowania z Internetu wszelkich utworów (programów komputerowych, utworów muzycznych, filmów, gier komputerowych, itp.), będących przedmiotem ochrony praw autorskich.
6. Naruszenia wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowią poważne naruszenie dyscypliny pracy.
7. Pracownicy nie mogą samodzielnie dokonywać zakupu oprogramowania.
8. Nośniki instalacyjne oprogramowania znajdują się w zamkniętej szafie lub na serwerze zasobów. Nośniki oprogramowania nie mogą być przechowywane w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden inny sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.
9. Przypadki instalowania i uruchamiania oprogramowania niedopuszczonego do użycia przez bibliotekę (w tym np. oprogramowania skopiowanego / pobranego własnoręcznie z Internetu), w szczególności, gdy jego uruchomienie wywołuje działania niedozwolone, po ich potwierdzeniu, będą podlegały szczegółowej analizie i mogą być traktowane jako celowe i świadome działanie zmierzające do zwiększenia ryzyka nieprawidłowego działania zasobów i sieci teleinformatycznej.

**§ 4. Zasady korzystania** **ze sprzętu komputerowego**

1. Sprzęt komputerowy powierza się pracownikom wyłącznie w celu wykonywania obowiązków służbowych.
2. W bibliotece Pracownikowi zabrania się korzystania ze sprzętu komputerowego, do którego Pracodawca nie jest uprawniony.
3. Zabrania się dokonywania bez autoryzacji osoby prowadzącej obsługę informatyczną w instytucji. zmian w ustawieniach systemowych komputerów, w szczególności: ustawień BIOS-u, ustawień systemu operacyjnego (w tym instalowania urządzeń), ustawień sieci teleinformatycznej.
4. Zabrania się samodzielnego otwierania obudowy komputera oraz innych części komputerowych (np. monitorów, drukarek, myszy).
5. Uprawnionymi do dokonywania czynności, o których mowa w ust. 4 i 5 na warunkach określonych warunkami gwarancji sprzętu, jest osoba prowadząca obsługę informatyczną w instytucji.
6. Pracownik, w którego dyspozycji pozostaje sprzęt komputerowy ma obowiązek wyłączyć go po zakończeniu pracy.
7. Korzystanie z nośników danych dopuszczalne jest po wcześniejszym sprawdzeniu ich programem antywirusowym.
8. Pracownik może samodzielnie:
9. wymienić toner, tusz, taśmę i inne materiały eksploatacyjne,
10. usunąć zakleszczony papier.
11. Zezwala się Pracownikom na korzystanie z przenośnego komputera służbowego poza miejscem pracy, na zasadach wymienionych w regulaminie urządzeń przenośnych.

**§ 5. Zasady korzystania** **z sieci komputerowej (Internet)**

1. Do sieci teleinformatycznej może być podłączony tylko sprzęt będący własnością Pracodawcy, z zastrzeżeniem ust. 2.
2. Inny sprzęt komputerowy podłączany jest wyłącznie za pomocą sieci bezprzewodowej i za zgodą kierownika jednostki.
3. Zabrania się samowolnego podłączania do sieci komputerów lub innych urządzeń.
4. W centrali biblioteki z wyłączeniem pomieszczeń socjalnych i sekretariatu zabrania się wykorzystywania gniazd elektrycznych do zasilania innych urządzeń niż:
5. komputery,
6. peryferia komputerowe,
7. niszczarki,
8. urządzenia do obsługi spotkań,
9. telefony stacjonarne,
10. zasilacze awaryjne.
11. W celu zapewnienia bezpieczeństwa mechanizmom sieci teleinformatycznej Urzędu oraz dla jej użytkowników Pracownikowi zabrania się dokonywania na niej działań o charakterze nielegalnym, a w szczególności:
12. umieszczania lub uruchamiania programów i innych obiektów niebezpiecznych, w tym „koni trojańskich" czy innych programów realizujących niepożądane lub wrogie działania,
13. skanowania sieci teleinformatycznej,
14. prowadzenia ataków, włamań, itp., innych czynności związanych z ingerencją w działanie lub zasoby sieci teleinformatycznej biblioteki, lub Internetu,
15. naruszania w jakikolwiek sposób bezpieczeństwa serwerów i ich bezawaryjnej pracy, a zwłaszcza logowania się do serwerów, jeżeli zakres obowiązków tego nie wymaga,
16. anonimowego wysyłania poczty elektronicznej z sieci teleinformatycznej biblioteki,
17. gromadzenia na stanowisku pracy, tj. stacji roboczej lub na zasobie dyskowym udostępnionym w sieci LAN, w dowolnej, cyfrowej formie materiałów lub treści niezgodnych z obowiązującym prawem lub naruszających dobre obyczaje,
18. uruchamiania programów z komputerowych nośników zewnętrznych, tj. z płyt CD/DVD lub nośników typu pendrive, itp.,
19. rozpowszechnia nielegalnych plików do Internetu, tj. przesyłania zdjęć, filmów, tekstów czy innych formatów plików.
20. Pracownikowi zakazuje się umożliwiania osobom postronnym dostępu do sieci teleinformatycznej biblioteki, np. umożliwienia pracy na identyfikatorach i hasłach Pracownika.
21. Zabrania się Pracownikom Urzędu wykonywania następujących czynności przy użyciu sprzętu i oprogramowania należącego do Pracodawcy:
22. korzystania z komputera służbowego do celów prywatnych,
23. wykorzystywania połączenia z siecią Internet do celów innych niż służbowe,
24. wysyłania wiadomości pocztowych (e-mail), typu reklamy, „łańcuszki szczęścia", pornograficznych, itp.,
25. logowania się w celach prywatnych lub komercyjnych na stronach WWW czy uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, komercyjnych, itp.,
26. używania w celach prywatnych lub komercyjnych komunikatorów internetowych w rodzaju Skype, Gadu-Gadu, Tlen, itp.,
27. korzystania z serwisów internetowych niezwiązanych z obowiązkami Pracownika, np. oferujących gry internetowe i losowe, hazard, prywatne aukcje, rozrywkę, prywatne listy dyskusyjne., itp.,
28. przetwarzania na komputerach materiałów, do których Pracodawca nie posiada praw autorskich,
29. korzystania z serwisów internetowych zawierających treści niecenzuralne lub jakiekolwiek łamiące prawo obowiązujące na terenie Rzeczpospolitej Polskiej,
30. instalowania i wykorzystywania jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności w bibliotece.
31. zapisywania, przechowywania na dyskach lokalnych lub zasobach sieciowych wszelkich plików multimedialnych niezwiązanych z wykonywaniem czynności służbowych,
32. używania sprzętu komputerowego poza siedzibami biblioteki bez zgody kierownika jednostki,
33. samodzielnej zmiany konfiguracji sprzętowej zestawu i jego ustawień systemowych,
34. udostępniania innym użytkownikom haseł dostępowych i ich przechowywanie w łatwo dostępnych lub widocznych miejscach,
35. używania nośników danych nieznanego pochodzenia oraz nośników wymiany pamięci z wyłączenie obsługi czytelnika książki mówionej.
36. każdej usterce sprzętu należy powiadomić pracownika odpowiedzialnego za obsługę informatyczną. Za dane i wykonywanie kopii danych przechowywanych na dyskach lokalnych odpowiada użytkownik zestawu komputerowego.

**§ 6.** **Procedury kontrolne oraz zastosowane zabezpieczenia dotyczące komputerowego stanowiska pracy w Bibliotece**

1. Wszelkie czynności pracownika w zakresie działań pracodawcy zmierzających do poprawy jakości pracy z komputerem polegające, w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążeniu sieci informatycznej, poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnych treści oraz kontroli antywirusowej związane są bezpośrednio z bezpieczeństwem biblioteki i ochroną danych osobowych, będą monitorowane.
2. Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych będzie przeprowadzone na bazie dedykowanego oprogramowania, będącego własnością pracodawcy, który posiada do niego stosowaną licencję.
3. Opis wprowadzonych zabezpieczeń sieci teleinformatycznej oraz komputerów w bibliotece:
4. regularne przeglądy logów systemów (nie rzadziej niż raz na 6 miesięcy);
5. kontrola zdarzeń na komputerze użytkownika;
6. przesyłanie alertów na komputer pracownika przez administratora sieci informatycznej;
7. monitoring używanych przez pracownika aplikacji;
8. blokada zbędnych aplikacji, lub stron internetowych;
9. blokada możliwości nagrywania płyt CD/ DVD
10. monitoring odwiedzanych przez pracowników stron internetowych;
11. monitoring ruchu w sieci informatycznej (LAN);
12. monitoring legalności oprogramowania;
13. monitoring służbowych kont poczty e-mail. Pracodawca zastrzega sobie prawo do kontroli treści wysłanych i otrzymanych e-maili z konta służbowego;
14. monitoring używania przenośnych nośników danych (pendrive, karty pamięci, CD-ROM, HDD, itp.) z możliwością blokowana, jak i odczytania ich treści;
15. blokada możliwości uruchomienia nieznanego pendrive’a.

**Załącznik nr 9c do Polityki Ochrony Danych**

**Regulamin korzystania ze służbowej poczty elektronicznej**

**§ 1. Główne zasady korzystania ze służbowej poczty elektronicznej**

1. Użytkownicy służbowej poczty elektronicznej powinni korzystać z poczty elektronicznej

mając na uwadze zagrożenia i ryzyka z tym związane.

1. Placówka posiada trzy rodzaje kont służbowych:
2. kierownicze utworzone zgodnie ze wzorem - pierwsza litera imienia, nazwisko: nazwisko@biblioteka.wloclawek.pl ,
3. działowe utworzone zgodnie ze wzorem - nazwa działu: nazwadzialu@biblioteka.wloclawek.pl ,
4. przypisane do filii utworzone zgodnie ze wzorem - nazwa filii i jej numer: nazwafiliinumer@biblioteka.wloclawek.pl .
5. Do głównych ryzyk związanych z korzystaniem ze służbowej poczty elektronicznej należą:
6. przekazanie wiadomości elektronicznej do nieuprawnionego odbiorcy, a także przechwycenie, odczytanie, zapisanie, dalsze przekazanie wiadomości elektronicznej przez nieuprawnionego odbiorcę,
7. wysyłanie wiadomości do wielu odbiorców w sposób ujawniający pozostałym ich tożsamość (pozwalający na identyfikację osoby fizycznej), a także adres poczty elektronicznej i temat korespondencji,
8. niewłaściwe treści zawarte w wiadomości elektronicznej lub załącznikach mogące stanowić uzasadnienie dla odpowiedzialności prawnej.

**§ 2.** **Zasady korzystania ze służbowej poczty elektronicznej przez pracowników Biblioteki**

1. Korzystanie ze służbowej poczty elektronicznej jest jednym ze sposobów realizowania obowiązków powierzonych Użytkownikowi poczty i powinno być realizowane tylko i wyłącznie w celach służbowych, związanych z realizowaniem tych zadań.
2. Użytkownicy służbowej poczty elektronicznej są zobowiązani do korzystania z poczty elektronicznej w taki sposób, aby minimalizować ryzyka naruszenia bezpieczeństwa informacji i ochrony danych osobowych.
3. Użytkownicy służbowej poczty elektronicznej ponoszą odpowiedzialność za działania podejmowane z wykorzystaniem przydzielonego konta pocztowego.
4. Kierownicze konto służbowe pocztowe jest imienne oraz przypisane do tożsamości Użytkownika przez cały okres funkcjonowania tego konta (zatrudnienia u Pracodawcy).
5. Okres przysługiwania uprawnień do służbowego konta pocztowego odpowiada okresowi pozostawania przez Użytkownika w zatrudnieniu u Pracodawcy.
6. Z imiennych kont pocztowych służbowego systemu poczty elektronicznej funkcjonującego u Pracodawcy może korzystać wyłącznie Użytkownik, dla którego konto pocztowe zostało założone. Zabronione jest udzielanie dostępu do służbowego konta pocztowego innym Użytkownikom.
7. Zabronione jest korzystanie ze służbowego adresu e-mail innego Użytkownika, a także logowanie się do skrzynki pocztowej innego Użytkownika.
8. Wszystkie nieprawidłowości w działaniu służbowej poczty elektronicznej, a także wątpliwości związane ze sposobem korzystania z poczty elektronicznej, w tym związane z jej bezpieczeństwem, należy niezwłocznie konsultować z pracownikiem odpowiedzialnym u Pracodawcy za obsługę informatyczną.
9. Dane osobowe lub informacje poufne przekazywane drogą elektroniczną powinny być przekazywane w załączniku zabezpieczonym hasłem, zgodnie z procedurą opisaną w regulaminie.
10. Kontrola wolnego miejsca w służbowej skrzynce pocztowej w ramach przyznanej przestrzeni dyskowej leży po stronie Pracownika.
11. Wiadomości, które nie wymagają przechowywania w celu ich przyszłego wykorzystania powinny być przez Pracownika regularnie usuwane ze skrzynki pocztowej.
12. Pracownik jest zobowiązany do samodzielnego archiwizowania zawartości swojego służbowego konta pocztowego.
13. Pracodawca nie ponosi odpowiedzialności za utracone wiadomości poczty elektronicznej.

**§ 3. Obowiązki pracowników Biblioteki w zakresie korzystania ze służbowej poczty elektronicznej**

1. Korzystanie ze służbowej skrzynki pocztowej założonej indywidualnie dla każdego Kierownika, któremu jest to niezbędne do wykonywania obowiązków służbowych, jest jego obowiązkiem.
2. Korzystanie ze służbowej skrzynki pocztowej założonej na dział / filię , któremu jest to niezbędne do wykonywania obowiązków służbowych, jest jego obowiązkiem.
3. Pracownik jest zobowiązany do korzystania z przyznanego mu służbowego adresu poczty elektronicznej do prowadzenia wszelkiej korespondencji służbowej z innymi Pracownikami placówki oraz instytucjami, z którymi współpracuje jednostka.
4. Pracownik jest zobowiązany do korzystania z przyznanego mu służbowego adresu poczty elektronicznej do prowadzenia korespondencji zewnętrznej prowadzonej w imieniu Pracodawcy, jeżeli wynika to z powierzonych obowiązków służbowych oraz w zakresie tego powierzenia.
5. Przy korespondencji Pracownik zobowiązany jest do:
6. sprawdzania skrzynki pocztowej przynajmniej raz dziennie każdego dnia, w którym jest obecny w pracy i wykonuje obowiązki służbowe;
7. bezzwłocznego odpowiadania na e-maile;
8. podawania tematu e-maila oraz umieszczania swojego podpisu.
9. Pracownik zobowiązuje się, że nie będzie działał w sposób naruszający prawa innych Użytkowników systemu pocztowego oraz nie będzie przenosił prawa do korzystania ze swojej skrzynki pocztowej na osoby trzecie.
10. Pracownik ma prawo korzystać ze służbowego konta pocztowego w pełnym zakresie jego funkcjonalności pod warunkiem, że będzie to zgodne z obowiązującym prawem, normami społecznymi i obyczajowymi.
11. Pracownik powinien stosować odpowiednie środki ostrożności zapobiegające wprowadzeniu wirusów do systemu poczty elektronicznej.

**§ 4****. Uprawnienia i obowiązki Pracodawcy w zakresie służbowej poczty elektronicznej**

1. Pracodawca zastrzega sobie prawo do:
2. awaryjnego wyłączenia systemu bez uprzedniego powiadomienia Użytkowników o tym fakcie,
3. zmiany zasad funkcjonowania systemu poczty elektronicznej, a informacje o tym fakcie będą podawane do wiadomości Pracownikom za pomocą poczty elektronicznej;
4. zamykanie kont pocztowych osób, które przestają być pracownikami placówki,
5. zablokowania skrzynek pocztowych w przypadkach wykorzystania ich w sposób niezgodny z przeznaczeniem i szeroko rozumianym interesem Pracodawcy. W szczególności może to dotyczyć:
6. wykorzystania skrzynek pocztowych do prywatnej działalności komercyjnej,
7. zachowań naruszających zasady wymienione w niniejszym dokumencie,
8. zachowań naruszających inne zasady i regulaminy użytkowania sieci komputerowych oraz naruszających ogólnie przyjęte zasady współistnienia użytkowników sieci Internet.
9. Zawartość konta pocztowego może zostać udostępniona na wezwanie uprawnionego organu państwowego, jeżeli obowiązek taki wynika z powszechnie obowiązujących przepisów prawa.

**§ 5. Konfigurowanie wiadomości**

1. Przed wysłaniem pierwszej wiadomości z systemu poczty elektronicznej Użytkownik jest zobligowany do skonfigurowania zasad wysyłania wiadomości, w tym nazwy Użytkownika i podpisu pod wiadomością zgodnie z obowiązującymi w organizacji standardami (podpis stanowi podanie imienia i nazwiska Pracownika obsługującego dane konto, stanowiska służbowego, nazwy i siedziby Pracodawcy, adresu strony www, numeru telefonu głównego Pracodawcy).
2. W przypadku nieobecności Użytkownika należy ustawić „autoodpowiedź" zawierającą informację o osobie, która go zastępuje w czasie nieobecności, do której nadawca może przekazać wiadomość.
3. Ustawienie przekazywania wiadomości na inny adres e-mail, tzn. innego Pracownika, wymaga uprzedniej zgody bezpośredniego przełożonego. Zgoda powinna być udokumentowana (na piśmie lub elektronicznie, jako wiadomość e-mail).
4. Jeżeli kilku Pracowników korzysta z ogólnego adresu e-mail, np. kontakt@, to każda wiadomość powinna zostać podpisana co najmniej imieniem i nazwiskiem osoby, która udziela odpowiedzi.
5. Użytkownik przyjmuje do wiadomości, że w przypadku zakończenia współpracy, może zostać ustawiona na jego koncie e-mail autoodpowiedź informująca o zakończeniu współpracy i adresie e-mail osoby, która go zastąpi.
6. Każda wiadomość powinna być wysyłana z zachowaniem należytej staranności w zakresie sprawdzenia poprawności treści, załączników, a w szczególności adresatów wiadomości.
7. Zalecane jest okresowe czyszczenie skrzynki pocztowej poprzez usuwanie starych wiadomości, które nie będą już potrzebne oraz przechowywanie wiadomości w strukturze folderów.

**§ 6. Przesyłanie danych osobowych**

1. Użytkownik może zastosować szyfrowanie wiadomości wewnętrznych w przypadku przesyłania treści objętych szczególną ochroną, z uwzględnieniem wcześniejszej wymiany certyfikatów pomiędzy nadawcą i odbiorcą (np. przez przesłanie wiadomości podpisanych cyfrowo). Zasady szyfrowania korespondencji zewnętrznej powinny być uzgadniane z poszczególnymi odbiorcami.
2. Dane osobowe (w szczególności imiona, nazwiska, adresy e-mail) lub inne informacje poufne nie powinny być wpisane w treść e-maila, a powinny zostać przekazywane w zabezpieczonym hasłem załączniku do wiadomości e-mail.
3. Dane osobowe (w szczególności imiona, nazwiska, adresy e-mail) lub inne informacje poufne nie mogą stanowić tematu e-maila.
4. Użytkownik może także zabezpieczyć plik lub pliki poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem. Ochrona przesyłanych plików może być również realizowana w powiązaniu z klasyfikacją informacji poprzez opatrzenie dokumentu odpowiednim hasłem wymaganym do otwarcia i/lub modyfikacji.
5. Hasło powinno być odpowiednio skomplikowane i nie słownikowe.
6. Hasło powinno zostać przekazane odbiorcy innym kanałem komunikacji (inną drogą korespondencji) niż wiadomość e-mail z załącznikiem.
7. Dopuszczalne jest uzgodnienie stałego hasła na korespondencję z jednym odbiorcą.
8. W korespondencji z danym odbiorcą dopuszczalne jest zastosowanie jako hasła konkretnej informacji znanej tylko temu odbiorcy, której nie trzeba będzie przekazywać odrębną drogą komunikacji, np. znany mu numer ewidencyjny.

**§ 7. Działania zakazane**

1. Za niedozwolone użycie systemu poczty elektronicznej Pracodawcy uznaje się jakiekolwiek świadome lub nieświadome użycie systemu poczty elektronicznej Pracodawcy prowadzące do naruszenia regulaminu, dobrego imienia Pracodawcy oraz osób trzecich lub naruszenia powszechnie obowiązujących przepisów prawa. W szczególności, za działania niedozwolone uznaje się:
2. działania skutkujące naruszeniem dóbr osobistych innych osób, w tym innych użytkowników,
3. tworzenie, wysyłanie lub przechowywanie wiadomości e-mail lub załączników, które mogą być uznane za nielegalne lub są powszechnie uznawane za obraźliwe, nieetyczne, nielegalne lub w inny sposób niestosowne, dotyczy to w szczególności: obraźliwych komentarzy dotyczących rasy, płci, koloru skóry, niepełnosprawności, wieku, orientacji seksualnej, pornografii, terroryzmu, przekonań i praktyk religijnych, przekonań politycznych, narodowości, odnośników do ewidentnie lub ewentualnie obraźliwych stron WWW i podobnych materiałów,
4. wykorzystanie systemu poczty elektronicznej Pracodawcy w celu rozsyłania spamu lub zakłócania pracy innych usług, w tym rozsyłanie żartów, wiadomości typu „łańcuszki”, próśb o pomoc charytatywną, wirusów i innego złośliwego oprogramowania,
5. używanie poczty elektronicznej do oficjalnego reprezentowania Pracodawcy, jeżeli nie wynika to z zakresu przydzielonych obowiązków służbowych albo z uzyskanego odpowiedniego upoważnienia,
6. wykorzystanie systemu poczty elektronicznej Pracodawcy w celach prowadzenia przez Pracownika działań politycznych oraz do prowadzenia własnej działalności gospodarczej,
7. używanie poczty elektronicznej do korespondencji prywatnej lub pracy charytatywnej niepowiązanej z realizowaniem obowiązków służbowych przydzielonych Pracownikowi ani działalnością Pracodawcy,
8. wysyłania wiadomości e-mail z cudzego konta lub w cudzym imieniu (włączając w to użycie zmienionego pola „Od:”/ ang. „From:”),
9. udostępnianie lub umożliwienie dostępu do własnego konta pocztowego innym osobom,
10. każde inne użycie poczty elektronicznej w nieetycznym celu lub niezgodne z prawem.
11. Zabronione jest używanie poczty elektronicznej do ręcznego wysyłania masowej korespondencji – w takiej sytuacji powinien zostać zastosowany specjalny program do zbiorczego mailingu.
12. Zabronione jest uczestniczenie w przechwytywaniu, podglądaniu, zapisywaniu, zmienianiu lub ujawnianiu wiadomości e-mail należącej do innej osoby (nie dotyczy osób odpowiednio Regulamin korzystania ze służbowej poczty elektronicznej upoważnionych lub wtedy, gdy niezbędne jest to do zarządzania systemem poczty elektronicznej).
13. Zabrania się korzystania w celach służbowych z innej, w tym prywatnej poczty e-mail.
14. Zabronione jest przekierowywanie (tzw. „forward” i „auto-forward”) wiadomości elektronicznych do innych, zewnętrznych systemów pocztowych.

**Załącznik nr 9d do Polityki Ochrony Danych**

**Polityka haseł**

1. Polityka haseł Miejskiej Biblioteki Publicznej im. Zdzisława Arentowicza we Włocławku określa zasady tworzenia haseł dostępowych użytkowników systemu operacyjnego Windows, oprogramowania SowaSQL, programu Comarch ERP Optima oraz programu Płatnik.
2. W jednostce hasła Administratora Systemów Informatycznych (ASI) przechowywane są w zapieczętowanej kopercie, w szafie pancernej oraz zmieniane na nowe co 30 dni kalendarzowe.
3. W jednostce funkcjonują trzy typy komputerowych kont pracowniczych:
4. administrator,
5. zwykły pracownik,
6. zastępstwo.
7. Tworzone przez użytkownika hasło dostępowe musi spełniać następujące wymagania:
8. konto administratora:
9. hasło nie może zawierać nazwy konta użytkownika,
10. hasło powinno zawierać:
* minimum 9 znaków,
* 2 znaki specjalne,
* cyfrę,
1. jeśli jest to możliwe włączone uwierzytelnianie dwuskładnikowe,
2. hasło nie może zawierać nazwy konta użytkownika,
3. hasło dostępowe nie będzie mogło zawierać znaków dwuznacznych:
* l (małe L),
* I (duże i),
* | (SHIFT + \),
* 0 (zero),
* O (duże o).
1. hasło musi zawierać jeden znak z wszystkich kategorii:
* wielkie litery,
* małe litery,
* cyfry,
* znaki specjalne (np.: !@#$\_^&%).
1. konto zwykłego pracownika oraz zastępstwo:
2. długość hasła: minimum 8 znaków,
3. hasło nie może zawierać nazwy konta użytkownika,
4. hasło dostępowe nie będzie mogło zawierać znaków dwuznacznych:
* l (małe L),
* I (duże i),
* | (SHIFT + \),
* 0 (zero),
* O (duże o).
1. hasło musi zawierać jeden znak z wszystkich kategorii:
* wielkie litery,
* małe litery,
* cyfry,
* znaki specjalne (np.: !@#$\_^&%).
1. Jeżeli system lub oprogramowanie czy usługa internetowa nie wymusza zmiany hasła, pracownicy powinni samodzielnie zmieniać hasło.
2. Użytkownik komputera, który odchodzi od swojego stanowiska pracy zobowiązany jest do aktywacji blokady (klawisz z logo systemu Windows + L).
3. Użytkownik jest zobowiązany zmienić hasło we wszystkich posiadanych kontach co najmniej jeden raz w przeciągu kolejnych 30 dni kalendarzowych czyniąc to samodzielnie według schematu zmiany haseł.
4. Nowo utworzone hasło nie może być wykorzystane w przeciągu 365 dni.
5. Hasło nie powinno kojarzyć się w żaden sposób z użytkownikiem (należy unikać imion, nazwisk rodziny, dzieci i znajomych, dat urodzenia, numerów telefonów).
6. Hasło nie powinno kojarzyć się z otoczeniem użytkownika (należy unikać imion zwierząt domowych, adresu, numeru rejestracyjnego lub nazwy samochodu).
7. Pracownik pracujący na zastępstwo otrzyma nowe hasło do konta zastępstwo.
8. Nie należy stosować nazw znanych postaci literackich, filmowych czy z bajek.
9. Należy unikać słów w brzmieniu słownikowym (również w języku angielskim i w językach powszechnie znanych).
10. Nie należy stosować wyrazów złożonych z sekwencji odczytywanej z klawiatury (np. asdfgh, qwerty).
11. Nie należy używać haseł złożonych z samych cyfr lub z takich samych liter.
12. Nie zaleca się używania w hasłach polskich znaków diakrytycznych, takich jak ę, ó, ą, ś, ł, ż, ź, ć, ń.
13. Można stosować kilka słów bez polskich znaków diakrytycznych połączonych w jeden wyraz.
14. Nie należy używać tego samego hasła dla wielu różnych celów.
15. Nie należy haseł zapisywać na kartkach, ani naklejać na komputer / monitor, pod klawiaturę czy w szufladzie.
16. Nie należy zapisywać haseł w przeglądarkach internetowych (np. poczty Zenbox).
17. Nie należy haseł przekazywać innym osobom oraz administratorom.
18. W przypadku ujawnienia hasła musi być ono niezwłocznie zmienione.
19. Zmianę hasła do systemu operacyjnego użytkownik może przeprowadzić samodzielnie.
20. Zmianę hasła do poczty elektronicznej Zenbox użytkownik może przeprowadzić samodzielnie według poniższego schematu:
21. Należy zalogować się do poczty poprzez przeglądarkę internetową,
22. Wejść do ustawień,
23. Hasło,
24. Aby zmienić hasło należy wpisać dotychczasowe hasło a następnie nowe i potwierdzenie nowego hasła,
25. Kliknąć zapisz.

**Załącznik nr 9e do Polityki Ochrony Danych**

**Procedura nadawania i usuwania uprawnień do systemów informatycznych wykorzystywanych w Bibliotece**

**(Sowa SQL Premium, Comarch ERP Optima oraz Płatnik)**

**§ 1. Nadawanie Uprawnień do systemów informatycznych**

1. Nadanie uprawnień (utworzenie konta) następuje po podpisaniu umowy o pracę, umowy zlecenia itp. pomiędzy Miejską Biblioteką Publiczną im. Zdzisława Arentowicza we Włocławku, a pracownikiem / przedsiębiorcą / usługodawcą.
2. Uprawnienia przyznawane są tylko na czas trwania umowy, czy usługi.
3. Utworzenie konta w systemie informatycznym wykorzystywanym w Bibliotece następuję po:
4. podpisaniu przez obie strony umowy,
5. podpisaniu uprawnień przez kierownika jednostki,
6. nadaniu identyfikatora użytkownika,
7. utworzeniu jednorazowego hasła dostępowego.
8. Nowo utworzone konto posiada jednorazowe hasło, które należy zmienić po pierwszym logowaniu do programu. Jeżeli do utworzenia konta w systemie informatycznym wykorzystywanym w bibliotece wymagany jest kontakt z dostawcą systemu następuje on w dniu podpisania umowy.

**§ 2. Tymczasowe zawieszenie konta użytkownika**

1. Tymczasowe zawieszenie konta użytkownika następuje w wyniku nieobecności w pracy / niezdolności do wykonywania obowiązków służbowych trwającej powyżej 21 dni roboczych / kalendarzowych.
2. Po powrocie do pracy użytkownik otrzymuje jednorazowe hasło do konta, które należy zmienić po pierwszym logowaniu do programu.

**§ 3. Odbiór uprawnień do systemów informatycznych**

1. Odbiór uprawnień do systemów informatycznych wykorzystywanych w bibliotece następuje następnego dnia roboczego po ustaniu stosunku pracy, wygaśnięcia umowy lub zmiany stanowiska pracy.
2. Jeżeli do usunięcia konta w systemie informatycznym wykorzystywanym w bibliotece wymagany jest kontakt z dostawcą systemu następuje on następnego dnia roboczego po ustaniu stosunku pracy, wygaśnięcia umowy lub zmiany stanowiska pracy.

**Załącznik nr 9f do Polityki Ochrony Danych**

**Procedura utylizacji i likwidacji nośników danych**

1. Utylizacja , likwidacja nośników danych wykorzystanych w Miejskiej Bibliotece Publicznej im. Zdzisława Arentowicza we Włocławku odbywa się nie rzadziej niż co 2 lata lub przy zebranej ilości 10 sztuk nośników danych.
2. Proces odbywa się według następujących kroków:
3. demontaż nośnika HDD / SSD z komputera stacjonarnego / laptopa; odbiór pendrive’a od pracownika,
4. spisanie protokołu utylizacyjnego przez komisję tj. spisanie nr seryjnego, nazwę producenta, nazwę serii,
5. dokonanie mechanicznego / fizycznego uszkodzenia danych poprzez uszkodzenia złącza do podłączenia nośnika oraz przewiercenie nośnika wiertłem przy obecności komisji,
6. przechowanie nośników danych w zabezpieczonych pomieszczeniach,
7. zamówienie usługi demagnetyzacji nośników danych,
8. możliwe jest również zamówienie zniszczenia nośnika danych w niszczarce,
9. otrzymanie protokołu z dokonanej usługi,
10. przekazanie nośnika lub jego pozostałości do utylizacji.

**Załącznik nr 2.4 do Polityki Ochrony Danych**

**Klauzula informacyjna – monitoring wizyjny**

Informujemy, że w celu zapewnienia bezpieczeństwa pracowników Biblioteki, ochrony mienia oraz zapewnienia porządku publicznego i bezpieczeństwa użytkowników Biblioteki, a także ochrony przeciwpożarowej na terenie Biblioteki realizowany jest monitoring wizyjny przy użyciu urządzeń rejestrujących.

Obszar objęty zasięgiem kamer monitoringu wizyjnego to: wejście główne, wyjście ewakuacyjne, wejście do piwnicy, wejście do Mediateki, Mediateka, strefa dziecka, sala kameralna, schody (piętro I i II), sala konferencyjna, wypożyczalnia (piętro I i II), czytelnia, magazyn książki, magazyn prasy, pomieszczenia biurowe (piętro I i II); łącznie 24 kamery.

Nagrania są gromadzone w sposób ciągły, ale ich przetwarzanie polegające na dokonywaniu podglądu zapisów realizowane jest dopiero w przypadku zdarzenia zagrażającego, bądź naruszającego dobra wskazane powyżej.

Nagrania udostępnianie są jedynie upoważnionym organom w trybie i na zasadach przewidzianych odrębnymi przepisami.

Nagrania przechowywane są przez 30 dni; po tym okresie nagrania są automatycznie kasowane. Dostęp do pomieszczeń, w których znajdują się rejestratory oraz monitory jest reglamentowany, a drzwi do pomieszczeń zamykane na klucz.

Administratorem Pani/ Pana danych osobowych jest Miejska Biblioteka Publiczna im. Zdzisława Arentowicza we Włocławku z siedzibą przy ul. Warszawskiej 11/13.

Inspektorem Ochrony Danych jest Adrian Domanowski, z którym można się skontaktować przez e‑mail: iod.bibliotekawloclawek@gmail.com lub pisemnie na adres naszej siedziby, wskazany powyżej.

Dane osobowe będą przetwarzane w granicach określonych przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) i ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz.U. z 2019r. poz. 1781).

Podstawą prawną korzystania z systemu monitoringu wizyjnego przez Bibliotekę jest art. 222 § 1 Kodeksu Pracy (t.j. Dz. U. z 2023r., poz. 1465) wprowadzony art. 111 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst ogłoszony - Dz.U. z 2018r. poz. 1000) oraz art. 6 ust. 1 lit. e) RODO, bowiem przetwarzanie danych w takiej formie jest elementem niezbędnym do wykonania zadań realizowanych w interesie publicznym.

Pani/ Pana dane osobowe nie będą podlegały zautomatyzowanemu procesowi podejmowania decyzji lub profilowaniu.

Przysługuje Pani/ Panu prawo do: dostępu do danych, ich sprostowania, ograniczenia przetwarzania, usunięcia danych, prawo do wniesienia sprzeciwu wobec ich przetwarzania, a także prawo do przenoszenia danych. Przysługuje Pani/ Panu również prawo do wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, a w sytuacji, w której podstawą prawną przetwarzania danych była zgoda, prawo do cofnięcia przedmiotowej zgody.

**Załącznik nr 6a do Polityki Ochrony Danych**

**Rejestr Użytkowników Sowa SQL Premium**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **l.p.** | *imię i nazwisko użytkownika* | *ważność upoważnienia (tak/ nie)* | *identyfikator* | *Data przyznania uprawnień* | *Data ustania uprawień* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Załącznik nr 6b do Polityki Ochrony Danych**

**Rejestr Użytkowników systemów Comarch oraz Płatnik**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **l.p.** | *imię i nazwisko użytkownika* | *ważność upoważnienia (tak/ nie)* | *identyfikator* | *Data przyznania uprawnień* | *Data odbioru uprawień* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Załącznik nr 9g do Polityki Ochrony Danych**

**Dziennik Zdarzeń Systemu Informatycznego**

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:

1. w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
2. w przypadku konserwacji systemu – opis podjętych działań, wnioski.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Data i godzina zdarzenia | Opis zdarzenia | Podjęte działania/wnioski | Podpis |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Załącznik nr 9h do Polityki Ochrony Danych**

**Regulamin użytkowania komputerów przenośnych**

1. Pracownicy użytkujący komputery przenośne i upoważnieni do przetwarzania danych osobowych za ich pomocą, zobowiązani są do zapoznania się z niniejszym Regulaminem i zobowiązania się do jego przestrzegania.
2. Pracownicy w celu wykonywania obowiązków służbowych mogą przetwarzać dane osobowe poza obszarem przetwarzania wyłącznie za pomocą służbowych komputerów przenośnych. Na potrzeby przetwarzania danych osobowych za pomocą komputerów przenośnych składają stosowne oświadczenie (*załącznik nr 1*).
3. Upoważnienie do przetwarzania danych osobowych za pomocą komputera przenośnego poza obszarem przetwarzania wydaje Administrator Danych Osobowych, w formie pisemnej (*załącznik nr 2*).
4. Upoważnienie, o którym mowa w pkt 3 zostaje odnotowane w Ewidencji Użytkowników Komputerów Przenośnych (*załącznik nr 3*), która obejmuje co najmniej: datę wydania upoważnienia, nr identyfikacyjny komputera przenośnego, imię i nazwisko oraz stanowisko służbowe pracownika, datę ustania/odwołania upoważnienia i zwrotu komputera przenośnego.
5. Pracownik, któremu udostępniono komputer przenośny, nie ma prawa udostępniać sprzętu innej nieupoważnionej osobie, bez zgody Administratora Danych Osobowych.
6. Komputer przenośny wyposażony jest w oprogramowanie antywirusowe zabezpieczające system przez złośliwym oprogramowaniem, oraz przed nieuprawnionym dostępem do zasobów komputera z sieci zewnętrznej (Internet) poprzez tzw. firewall programowy.
7. Komputer przenośny nie jest wyposażony w oprogramowanie zabezpieczające m.in. od zdarzeń losowych typu kradzież, lub pozostawienie laptopa w miejscu ogólnodostępnym, poprzez zastosowanie mechanizmu szyfrującego dane na dysku komputera.
8. Opisane w pkt. 5 i 6 zabezpieczenia zobowiązują użytkownika komputera przenośnego do:
9. zachowania w tajemnicy loginu i hasła do logowania się do systemu operacyjnego,
10. nieingerowania w ustawienia programu antywirusowego zainstalowanego na komputerze przenośnym, w szczególności podejmowania próby wyłączania automatycznej aktualizacji bazy wirusów.
11. Pracownik korzystając z komputera przenośnego zobowiązuje się do przestrzegania następujących reguł postępowania:
	1. operacje wykonywane na komputerze przenośnym realizowane są wyłącznie w celach służbowych;
	2. połączenie z siecią Internet można uruchamiać wyłącznie w uzasadnionych przypadkach podyktowanych zakresem zadań służbowych, przy czym:
* użytkownik komputera uruchamia wyłącznie strony internetowe związane z wykonywaniem zadań służbowych,
* nie zapisuje w pamięci przeglądarki internetowej haseł dostępowych,
* nie pobiera, ani nie zatwierdza aktualizacji pojawiających się automatycznie w trakcie przeglądania stron;
	1. kopiowanie danych zapisanych na służbowym komputerze przenośnym jest możliwe wyłącznie na zewnętrzny zaszyfrowany nośnik typu pendrive zabezpieczony hasłem, udostępniony przez Administratora Danych Osobowych; zabronione jest wykorzystywanie na potrzeby przenoszenia danych/ sporządzania kopii danych prywatnych nośników zewnętrznych;
	2. wysyłanie danych osobowych lub danych poufnych jest możliwe wyłącznie za pomocą służbowej poczty elektronicznej w formie załączonego zaszyfrowanego pliku zabezpieczonego co najmniej 8-znakowym hasłem (duże, małe litery i cyfry), w tym celu można wykorzystać np. program „7 zip”.
1. Użytkownik komputera przenośnego ma obowiązek informowania Administratora Danych Osobowych o niepokojących monitach/komunikatach ze strony systemu/programu antywirusowego takich jak: brak możliwości wykonania aktualizacji bazy wirusów, informacje o próbach włamania, czy też informacje o wyryciu złośliwego oprogramowania.
2. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego
w czasie transportu, w szczególności do:
3. przenoszenia komputera przenośnego za pomocą torby / plecaka przeznaczonego do przechowywania i przenoszenia komputerów przenośnych,
4. nie przenoszenia komputera przenośnego w zwykłej teczce, aktówce,
5. nie pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.
6. Gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie go hasłem. Dotyczy to przede wszystkim zabezpieczenia komputera przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia.
7. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.
8. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem Administratorowi Danych Osobowych.

*Załącznik nr 1 do Regulaminu użytkowania komputerów przenośnych*

 Włocławek, dn. …………………..

………………………….…

 *(imię i nazwisko pracownika)*

……………………….……

 *(stanowisko służbowe)*

**Oświadczenie**

Oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych oraz bezpieczeństwa informacji w systemach informatycznych, w szczególności treść Polityki Ochrony Danych oraz, że zostałem zaznajomiony z rodzajami informacji stanowiących tajemnice służbową w Miejskiej Bibliotece Publicznej oraz regulaminami, instrukcjami i procedurami ich ochrony.

Na potrzeby wykonywania zadań służbowych za pomocą komputera przenośnego, zobowiązuję się do przetwarzania danych osobowych zgodnie z przepisami Polityki Ochrony Danych oraz zachowania w tajemnicy informacji, do których mam lub będę miał dostęp.

Zobowiązuję się przestrzegać postanowień Polityki Ochrony Danych oraz innych obowiązujących w Miejskiej Bibliotece Publicznej im. Zdzisława Arentowicza we Włocławku przepisów dotyczących ochrony danych osobowych oraz bezpieczeństwa informacji w systemach informatycznych. Wiadomościami stanowiące tajemnicę służbową, nie będą przeze mnie wykorzystywane i udostępniane do celów innych niż służbowe.

 Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za ciężkie naruszenie obowiązków pracowniczych

……………………………………..
 *(data i czytelny podpis pracownika)*

*Załącznik nr 2 do Regulaminu użytkowania komputerów przenośnych*

 Włocławek, dn. …………………..

**UPOWAŻNIENIE nr …/…**

Z dniem …………………….. upoważniam Panią/Pana ………………………….……………

stanowisko służbowe: …………………………………………………………….…………….

do przetwarzania danych osobowych za pomocą służbowego komputera przenośnego poza obszarem przetwarzania danych, wyłącznie w celu realizacji zadań służbowych.

W związku z powyższym powierzam Pani/Panu komputer przenośny o numerze identyfikacyjnym ……………………… i zobowiązuję Panią/Pana do przestrzegania obowiązującego w Miejskiej Bibliotece Publicznej im. Zdzisława Arentowicza we Włocławku „Regulaminu użytkowania komputerów przenośnych”.

Okres ważności

od: …………………………………………………………………………….

do: …………………………………………………………………………….

......................................................................................

*(podpis osoby uprawnionej do nadania upoważnienia)*

Przyjąłem do wiadomości.

......................................................................................

 *(podpis osoby, której udzielono upoważnienia)*

Odwołano dnia .............................................................

......................................................................................

*(podpis osoby uprawnionej do odwołania upoważnienia)*

*Załącznik nr 3 do Regulaminu użytkowania komputerów przenośnych*

**Ewidencja Użytkowników Komputerów Przenośnych**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L.p. | Data wydania upoważnienia | Nr identyfikacyjny komputera przenośnego | Imię i nazwisko oraz stanowisko służbowe pracownika | Datę ustania/odwołania upoważnienia  | Data zwrotu komputera przenośnego |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Załącznik nr 9i do Polityki Ochrony Danych**

**Rejestr umów powierzenia przetwarzania danych osobowych**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  L.p. | Numer umowy |  Data zawarcia umowy | Strona umowy | Zakres powierzenia |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Załącznik nr 9k do Polityki Ochrony Danych**

**Procedura postępowania w przypadku wystąpienia awarii**

**oraz plan ciągłości działania w obszarze kluczowych procesów**

**§ 1. Cel procedury**

Celem planu jest minimalizacja awarii w zakresie naruszenia systemów ochrony danych osobowych w funkcjonowaniu Miejskiej Biblioteki im. Zdzisława Arentowicza we Włocławku.

**§ 2. Awaria**

1. Za awarię systemu uznaje się zdarzenie zachodzące w chwili, w której system przestaje realizować usługi oczekiwane przez użytkownika. Błąd systemu, błędne zachowane systemu niezgodne ze specyfikacją.
2. Każda awaria ewidencjonowana jest w *Dzienniku Zdarzeń Systemu Informatycznego, który stanowi Załącznik nr 9g do Polityki Ochrony Danych*

**§ 3. Zdarzenia powodujące brak dostępności**

Zdarzeniami mogącymi mieć wpływ na brak dostępności do danych osobowych jest:

1. umyślne bądź nieumyślne działanie lub zaniechanie osób zatrudnionych w jednostce,
2. ingerencja osób trzecich (np. atak hackerski),
3. zdarzenia losowe, np. pożar, zanik zasilania, utrata dostępu do sieci internetowej.

**§ 4. Obowiązek zgłoszenia**

Każdy pracownik Biblioteki, współpracownik jest osobą uprawnioną do zgłoszenia awarii lub innego czynnika zewnętrznego powodującego brak dostępności do danych, danych osobowych, w celu zapewnienia minimalizacji wpływu awarii na funkcjonowanie zabezpieczenia jednostki.

**§ 5. Czynności podjęte w razie awarii**

1. W razie wystąpienia awarii lub innego czynnika zewnętrznego należy dokonać zgłoszenia o podejrzeniu awarii Dyrektorowi Biblioteki lub Administratorowi Systemów Informatycznych – osobie odpowiedzialnej za zabezpieczenie systemów informatycznych w jednostce.
2. Administrator Systemów Informatycznych:
3. weryfikuje zasadność zgłoszenia,
4. ustala źródła awarii w porozumieniu z pracownikiem lub współpracownikiem, który dokonał zgłoszenia,
5. określa skalę awarii,
6. dokonuje identyfikacji problemu oraz niezwłocznie dokonuje niezbędnej naprawy urządzenia lub/i próby przywrócenia funkcjonalności systemu,
7. przygotowuje urządzenie lub serwer zastępczy, jeśli jest to niezbędne do zabezpieczenia danych, w tym danych osobowych w jednostce,
8. określa, czy awaria bądź zdarzenie miało wpływ na przetwarzanie danych osobowych i czy dane osobowe przetwarzane w systemie zostały utracone, zmodyfikowane lub udostępnione osobom postronnym,
9. informuje Inspektora Ochrony Danych o awarii mającej wpływ na dane osobowe,
10. sporządza notatkę służbową lub raport i przekazuje Inspektorowi Ochrony Danych osobowych w związku z ewentualną koniecznością podjęcia działań naprawczych i zapobiegających,
11. W przypadku, jeżeli awaria następuje z uwagi na działanie podmiotu dostarczającego usługi zewnętrzne, Dyrektor Biblioteki dokonuje zgłoszenia awarii podmiotowi odpowiedzialnemu za usługę, w czasie przewidzianym zawartą umową.
12. Informacje o awarii są przekazywane wszystkim pracownikom przez Dyrektora Biblioteki lub Administratora Systemów Informatycznych z jednoczesną instrukcją postępowania, np. zapisywanie danych w formie papierowej, niekorzystanie z Internetu.
13. Jeżeli awarii nie można usunąć niezwłocznie, a do jej usunięcia niezbędna jest usługa podmiotu zewnętrznego, osoba odpowiedzialna za zabezpieczenie systemu informatycznego zawiadamia Dyrektora Biblioteki o takiej potrzebie, jednocześnie przekazuje informację pracownikom Biblioteki o szacowanym czasie przywrócenia systemów.

**§ 6. Przywrócenie pracy systemu**

1. Po przywróceniu pracy systemu należy dokonać testu systemu, który będzie polegał na:
2. zweryfikowaniu, czy awaria bądź zdarzenie miało wpływ na przetwarzanie danych osobowych,
3. zweryfikowaniu czy dane osobowe przetwarzane w systemie zostały utracone, zmodyfikowane lub udostępnione osobom postronnym.
4. Po zakończeniu procesu testowania systemów, Administratora Systemów Informatycznych:
5. sporządza protokół, podpisuje go i kopię przekazuje Dyrektorowi Biblioteki oraz Inspektorowi Ochrony Danych,
6. dokonuje analizy ryzyka w zakresie wpływu incydentu na naruszenia danych osobowych, a w przypadku, kiedy ryzyko naruszenia danych osobowych jest wysokie i w trakcie analizy ustali się, że doszło do wycieku danych, należy dokonać analizy ryzyka oceniającej: czy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych; w takim przypadku administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu oraz zawiadamia Prezesa UODO.

**§ 7. Plan ciągłości działania na wypadek pożaru**

1. Zgłaszanie incydentu.
2. pracownik, który zidentyfikował pożar niezwłocznie powiadamia straż pożarną pod numerem 112 oraz Dyrektora Biblioteki;
3. po uzyskaniu telefonicznego połączenia ze Strażą Pożarną należy wyraźnie podać: dokładny adres, nazwę obiektu lub jego części, w której powstał pożar, co się pali (np. pali się sala kameralna, wypożyczalnia, archiwum, czy komputer w pomieszczeniu biurowym itp.), czy istnieje zagrożenie życia ludzkiego, nr telefonu z którego się dzwoni i swoje nazwisko.
4. Działania awaryjne.
5. równocześnie z alarmowaniem Straży Pożarnej należy przystąpić do akcji ratowniczo-gaśniczej przy pomocy gaśnic i hydrantów znajdujących się w budynku;
6. do czasu przybycia jednostek Straży Pożarnej, kierownictwo akcją obejmuje Dyrektor Biblioteki lub w razie nieobecności dyrektora osoba przez niego upoważniona;
7. zasady uczestnictwa w gaszeniu pożaru: w pierwszej kolejności należy przeprowadzić ratowanie zagrożonego życia, ewakuację ludzi a następnie ewakuację mienia, w tym dokumentacji i kopii zapasowych, wyłączyć dopływ prądu elektrycznego do pomieszczeń objętych pożarem, nie wolno gasić wodą jak i również gaśnicą pianową instalacji i urządzeń elektrycznych będących pod napięciem, usunąć z zasięgu ognia wszelkie materiały palne, a w szczególności butle z gazami palnymi, naczynia z płynami łatwopalnymi, cenne materiały, maszyny, urządzenia itp., nie otwierać bez potrzeby drzwi, okien do pomieszczeń, w których powstał pożar, ponieważ dopływ powietrza sprzyja rozprzestrzenianiu się ognia, przestrzegać w czasie gaszenia zasad bezpieczeństwa, otwierając drzwi do pomieszczeń w których powstał pożar należy zachować szczególną ostrożność (ognie żgące), wskazane jest schowanie się za ścianę od strony klamki w drzwiach lub otwieranie zza drzwi, wchodząc do zadymionych pomieszczeń lub przechodząc przez nie, należy ograniczyć ilość wdychanych produktów spalania, poruszać się w pozycji pochylonej, jak najbliżej podłogi i zasłaniać usta, np. wilgotną chustką;
8. po przyjeździe jednostki Straży Pożarnej do pożaru udzielić niezbędnych informacji i podporządkować się decyzji Kierującego Działaniami Ratowniczymi w zakresie działalności ratowniczo – gaśniczej;
9. zabezpieczyć mienie pozostałe na pogorzelisku, do ukończenia akcji gaśniczej.
10. Przywrócenie działania tymczasowego / naprawa z wykorzystaniem tymczasowych metod:
11. jeśli zniszczeniu uległa infrastruktura IT – przejść do realizacji procedury opisanej w § 8.,
12. jeśli zniszczeniu uległy media, uruchomić ich ponowną dostawę (energia, Internet, telekomunikacja) – przejść do realizacji procedury opisanej w § 8. oraz § 9.,
13. jeśli zniszczeniu uległy pomieszczenia – organizacja tymczasowej lokalizacji Biblioteki, przeniesienie do wyznaczonych i zaplanowanych wcześniej lokalizacji i pomieszczeń – osoba odpowiedzialna – Dyrektor Biblioteki;
14. podanie informacji przez Dyrektora Biblioteki do wszystkich zainteresowanych o ewentualnych zmianach w adresie lokalizacji i procedurach operacyjnych.
15. Wznowienie działalności:
16. podjęcie działań mających na celu likwidację szkód odniesionych w wyniku pożaru; osoba odpowiedzialna – Dyrektor Biblioteki;
17. sprawdzenie poprawności funkcjonowania zabezpieczeń p.poż.;
18. powiadomienie pracowników, osób współpracujących i użytkowników o wznowieniu działalności;
19. podjęcie działań dyscyplinarnych w przypadku ujawnienia jako przyczyny pożaru zachowania pracownika;
20. organizacja szkolenia w zakresie ochrony p.poż. oraz zachowywania się w trakcie pożaru;
21. przeprowadzenie cyklicznych testów w zakresie pozorowanego pożaru wraz z oceną zachowania koordynatora oraz pracowników (nie rzadziej niż raz na rok).

**§ 8. Plan awaryjny na wypadek braku zasilania w sieci komputerowej**

1. W przypadku stwierdzenia braku zasilania w sieci komputerowej Dyrektor Biblioteki, Kierownik Działu Administracyjno-Organizacyjnego lub Administrator Systemów Informatycznych kontaktuje się z dostawcą energii elektrycznej.
2. Serwer podłączony jest do urządzenia UPS (*dużego*) wyposażonego w baterie wystarczające na ok. 30 minut pracy oraz drugiego urządzenia UPS (*małego*) z bateriami wystarczającymi na ok. 2 min pracy.
3. Administrator Systemów Informatycznych zobowiązany jest do ukończenia wszelkich prac na serwerze i bezpiecznego wyłączenia systemu.
4. Jednostki komputerowe pracowników Działu Księgowości (4 szt.) są podłączone do urządzeń UPS (*małych)* z bateriami wystarczającymi na ok. 2 min pracy.
5. Pozostałe jednostki komputerowe nie są podłączone do zasilacza awaryjnego UPS. Każdy pracownik Biblioteki wykorzystujący w swojej pracy systemy komputerowe zobowiązany jest do okresowego zapisywania efektów swojej pracy lub wykorzystywania funkcji autozapisu.

**§ 9. Plan awaryjny na wypadek utraty dostępu do sieci internetowej**

W przypadku utraty dostępu do sieci Internet, Administrator Systemów Informatycznych zgłasza awarię do dostawcy przedmiotowej usługi.

**Załącznik nr 9l do Polityki Ochrony Danych**

**Raport dla kierownika jednostki o stanie informatyki**

**Rok ……….**

|  |  |  |
| --- | --- | --- |
| Lp. |  |  |
| 1 | Oznaczenie administratora danych i adres jego siedziby | Dyrektor Miejskiej Biblioteki Publicznej im. Zdzisława Arentowicza we Włocławku, ul. Warszawska 11/13 87-800 Włocławek |
| 2 | Imię i nazwisko Administratora Danych |  |
| 3 | Wykaz czynności podjętych przez Administratora Systemów Informatycznych w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach |  |
| 4 | Data rozpoczęcia i zakończenia sprawdzania |  |
| 5 | Określenie przedmiotu i zakresu sprawdzenia |  |
| 6 | Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych |  |
| 7 | Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem |  |
| 8 | Wyszczególnienie załączników stanowiących składową część sprawozdania |  |
| 9 | Podpis Administratora Systemów Informatycznych |  |
| 10 | Data |  |