Załącznik Nr 1 do Polityki Bezpieczeństwa Informacji
Biblioteki Publicznej im. Zygmunta Jana Rumla
w Dzielnicy Praga-Południe m.st. Warszawy
z dnia 31.03.2021 r.

Instrukcja

Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych

w Bibliotece Publicznej im. Zygmunta Jana Rumla
w Dzielnicy Praga-Południe m.st. Warszawy

Warszawa, marzec 2026 r.

Spis treści

§ 1 Cel i zakres stosowania instrukcji

1. Niniejsza Instrukcja Zarządzania Systemami Informatycznymi („IZSI") określa zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Bibliotece. Celem Instrukcji jest zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych, w tym ochrony ich poufności, integralności i dostępności, a także minimalizowanie ryzyka przypadkowego lub nieuprawnionego ujawnienia, utraty, zniszczenia lub uszkodzenia danych.
2. Instrukcja ma zastosowanie do wszystkich pracowników i współpracowników Biblioteki, którzy posiadają uprawnienia dostępu do danych osobowych przetwarzanych w systemach informatycznych Administratora Danych, niezależnie od formy zatrudnienia lub współpracy.
3. Instrukcja stanowi Załącznik Nr 1 do Polityki Bezpieczeństwa Informacji. W sprawach nieuregulowanych Instrukcją stosuje się Politykę Bezpieczeństwa Informacji i obowiązujące przepisy prawa.

§ 2 Podstawa prawna instrukcji

Niniejsza Instrukcja została opracowana na podstawie następujących aktów prawnych i dokumentów normatywnych:

1. **Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)** z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

2. **Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** (Dz.U. z 2019, poz.1781 t.j.)

3. **Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych** (Dz.U. z 2024, poz. 773) „Krajowe Ramy Interoperacyjności".

4. **Norm PN-ISO/IEC 27001:2022** (zarządzanie bezpieczeństwem informacji) oraz norm powiązanych, w szczególności:

    a) **PN-ISO/IEC 27002:2022** – wytyczne dotyczące środków bezpieczeństwa,

    b) **PN-ISO/IEC 27005:2018** – zarządzanie ryzykiem bezpieczeństwa informacji,

    c) **PN-ISO/IEC 22301:2020** – zarządzanie ciągłością działania.

5. Odwołania do norm mają charakter dobrych praktyk i nie nakładają na Bibliotekę obowiązku ich certyfikacji.

6. Zadania związane z nadzorem nad przestrzeganiem przepisów o ochronie danych osobowych realizuje **Inspektor Ochrony Danych (IOD)**, wyznaczony na podstawie art. 37–39 RODO.
   Sprawowanie nadzoru nie oznacza, że IOD posiada dostęp do wszystkich danych osobowych — dostęp ten jest przyznawany jedynie w zakresie niezbędnym do wykonywania jego ustawowych obowiązków.

7. Najważniejszym celem Instrukcji jest zapewnienie bezpieczeństwa danych osobowych poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, adekwatnych do ryzyka związanego z ich przetwarzaniem, oraz ustanowienie jasnych zasad postępowania dla użytkowników systemów informatycznych.

§ 3 Definicje

Użyte w Instrukcji określenia oznaczają:

1. **IZSI** – Instrukcja Zarządzania Systemami Informatycznymi;
2. **Administrator Danych Osobowych („ADO")** – Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy, reprezentowanej przez Dyrektora;
3. **Inspektor Ochrony Danych („IOD")** – osoba wyznaczona przez Administratora Danych do wykonywania obowiązków określonych w art. 37–39 RODO;
4. **Administrator Systemów Informatycznych („ASI")** – osoba odpowiedzialna za funkcjonowanie, bezpieczeństwo oraz utrzymanie systemów informatycznych i infrastruktury technicznej Administratora Danych, w szczególności: systemów operacyjnych, sieci lokalnej, urządzeń sieciowych, serwerów, stacji roboczych i zabezpieczeń technicznych;
5. **Administrator Systemu Informatycznego SOWA SQL** – osoba odpowiedzialna wyłącznie za administrowanie systemem SOWA SQL w zakresie użytkowników i konfiguracji aplikacyjnej; osoba ta nie posiada uprawnień administracyjnych do systemów operacyjnych, sieci, domen ani sprzętu należącego do Administratora Danych oraz nie wykonuje zadań ASI;
6. **Użytkownik** – pracownik lub współpracownik, posiadający dostęp do systemu informatycznego na podstawie upoważnienia nadanego przez ADO lub osobę przez upoważnioną przez ADO;
7. **Identyfikator** – unikalny ciągu znaków przypisany do użytkownika systemu informatycznego, umożliwiający jednoznaczną identyfikację użytkownika;
8. **Hasło** – ciąg znaków znany wyłącznie użytkownikowi, służący do uwierzytelniania w systemie informatycznym;
9. **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione ani usunięte w sposób nieautoryzowany;
10. **Odbiorca danych** – każda osoba lub podmiot, któremu udostępniane są dane osobowe, z wyjątkiem osoby, której dane dotyczą, osób upoważnionych do przetwarzania

danych, podmiotów przetwarzających oraz organów publicznych otrzymujących dane w związku z prowadzonym postępowaniem na podstawie prawa;

11. **Osoba upoważniona do przetwarzania danych** – osoba, która otrzymała pisemne upoważnienie do przetwarzania danych osobowych od ADO;
12. **Przetwarzający** – osoba fizyczna lub prawna, organ publicznemu, jednostka organizacyjna lub inny podmiot, który przetwarza dane osobowe w imieniu ADO na podstawie umowy powierzenia zgodnej z art. 28 RODO;
13. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych;
14. **Serwisant** – osoba lub podmiot zajmujący się sprzedażą, instalacją, konfiguracją lub naprawą sprzętu komputerowego lub oprogramowania na podstawie upoważnienia ADO;
15. **Awaria systemu informatycznego** – stan niesprawności systemu informatycznego lub elementu infrastruktury IT, powodujący jego nieprawidłowe działanie lub całkowite unieruchomienie, przy czym definicja obejmuje wszystkie systemy wykorzystywane przez Bibliotekę, w tym system SOWA SQL, systemy operacyjne, usługi sieciowe, hostingi, serwery i stacje robocze;
16. **Awaria jednostkowa** – awaria o ograniczonym zakresie, dotyczącej pojedynczego użytkownika, pojedynczego stanowiska lub jednej funkcji systemu, niewpływającej na działanie usług w placówce;
17. **Awaria zwykła (operacyjna)** – awaria wpływająca na funkcjonowanie systemu informatycznego lub jego części w jednej placówce lub dla grupy użytkowników, mającej wpływ na realizację usług, ale niewyłączającej ich całkowicie i niebędąca awarią krytyczną;
18. **Awaria krytyczna** – awaria uniemożliwiająca świadczenie usług Biblioteki lub uniemożlwiająca działanie kluczowych funkcjonalności systemu informatycznego w co najmniej jednej lokalizacji Biblioteki, powodująca całkowite wstrzymanie obsługi czytelników lub niemożność korzystania ze zbiorów Biblioteki;
19. **BP lub Biblioteka** – Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy;
20. **Instruktor** – osoba odpowiedzialna za sprawy merytoryczne związane z funkcjonowaniem systemu bibliotecznego SOWA SQL.

§ 4 Obowiązki z zakresu ochrony danych osobowych

1. **Do obowiązków osób przetwarzających dane osobowe w systemach informatycznych należy:**

a) przetwarzanie danych osobowych wyłącznie w celach oraz zakresie wynikających z przydzielonych obowiązków służbowych oraz zgodnie z udzielonym upoważnieniem;
b) niezwłoczne zgłaszanie wszelkich podejrzeń lub przypadków naruszenia ochrony danych osobowych do przełożonego, Administratora Systemów Informatycznych (jeżeli dotyczy systemów informatycznych), oraz do Inspektora Ochrony Danych;
c) współpraca z ADO, ASI, Administratora SOWA SQL (jeżeli dotyczy), oraz IOD przy wyjaśnianiu okoliczności naruszenia, ograniczaniu jego skutków oraz wdrażaniu działań zapobiegawczych.

2. **Użytkownicy będący pracownikami są zobowiązani do udziału w szkoleniach:**
   a) wstępnych — przed dopuszczeniem do pracy związanej z dostępem do danych osobowymi;
   b) okresowych — dotyczących zmian w systemach informatycznych (np. aktualizacje, wymiana sprzętu), zmian wewnętrznych procedur oraz zmian przepisów o ochronie danych osobowych;
   c) dodatkowych — organizowanych w przypadku istotnych incydentów, wdrożenia nowych systemów lub zmian organizacyjnych.
3. **Do obowiązków osób zarządzających pracownikami należy:**
   a) wnioskowanie o nadanie, zmianę lub odebranie uprawnień do systemów informatycznych, w których przetwarzane są dane osobowe, zgodnie z procedurą nadawania uprawnień;
   b) nadzorowanie czy pracownicy przetwarzają dane osobowe zgodnie z nadanymi uprawnieniami i zakresem obowiązków;
   c) zgłaszanie do ASI lub Administratora SOWA SQL (jeżeli dotyczy) konieczności modyfikacji lub odebrania uprawnień np. w przypadku zmiany stanowiska, reorganizacji pracy, nieobecności długoterminowej lub zakończenia współpracy.

4. **W przypadku powierzenia obsługi informatycznej podmiotowi zewnętrznemu lub w przypadku korzystania z systemów informatycznych zlokalizowanych w środowisku dostawcy zewnętrznego:**
   a) infrastruktura oraz środowisko systemowe podmiotu zewnętrznego muszą zapewniać poziom bezpieczeństwa nie niższy niż określony w niniejszej Instrukcji oraz w przepisach prawa;
   b) współpraca z podmiotem zewnętrznym odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych lub innych dokumentów regulujących bezpieczeństwo danych (zgodnie z art. 28 RODO);
   c) zakres dostępu oraz uprawnień osób działających po stronie podmiotu zewnętrznego jest ograniczony wyłącznie do celów realizacji zadań określonych umową i nadzorowany przez ASI lub Administratora Systemu, którego usługa dotyczy.

§ 5 Obowiązki Administratora Systemów Informatycznych

Do obowiązków Administratora Systemów Informatycznych, w których przetwarzane są dane osobowe, należy:

1. **Przestrzeganie procedur operacyjnych i procedur bezpieczeństwa** wynikających z niniejszej Instrukcji, Polityki Bezpieczeństwa Informacji oraz innych dokumentów wewnętrznych.
2. **Zarządzanie infrastrukturą informatyczną** Biblioteki w sposób zapewniający poufność, integralność i dostępność danych osobowych, w szczególności poprzez właściwą konfigurację, aktualizację i zabezpieczenie systemów operacyjnych, sieci, serwerów, usług domenowych i stacji roboczych.
3. **Zarządzanie systemowymi środkami uwierzytelniania**, w tym:
    - zakładanie kont,
    - blokowanie lub usuwanie kont,
    - modyfikowanie uprawnień,

    wyłącznie na podstawie prawidłowo zaakceptowanych wniosków złożonych przez osoby uprawnione.
4. **Utrzymanie systemów informatycznych w odpowiednim stanie technicznym**, obejmującym aktualizacje, poprawki bezpieczeństwa, kontrolę dostępności usług oraz monitorowanie działania infrastruktury.
5. **Nadzorowanie przepływu informacji pomiędzy systemami informatycznymi Biblioteki a siecią publiczną**, w tym zapewnienie ochrony na styku z Internetem (zabezpieczenia brzegowe, polityki firewall, filtrowanie ruchu i innych środków bezpieczeństwa).
6. **Nadzorowanie bezpieczeństwa systemów informatycznych**, w tym:
    - monitorowanie incydentów bezpieczeństwa,
    - analizowanie logów systemowych,
    - wykrywanie nieprawidłowości,
    - reagowanie na zgłoszenia użytkowników,
    - współpraca z IOD w zakresie naruszeń ochrony danych osobowych.
7. **Tworzenie i utrzymywanie kopii zapasowych** danych oraz oprogramowania, zgodnie z harmonogramem i zasadami określonymi w Instrukcji, a także **okresowa weryfikacja poprawności wykonywania kopii oraz zdolności do ich odtwarzania**.
8. **Nadzorowanie lub wykonywanie okresowej konserwacji systemów informatycznych**, w tym:
    - sprzętu komputerowego,
    - urządzeń sieciowych,
    - aplikacji systemowych,
    - elektronicznych nośników informacji,

    na których przetwarzane są dane osobowe.

9. **Współpraca z podmiotami zewnętrznymi** realizującymi usługi serwisowe, hostingowe lub outsourcingowe, w zakresie niezbędnym do utrzymania systemów informatycznych w bezpiecznym stanie.
10. **Zapewnienie, aby czynności techniczne ASI nie obejmowały odpowiedzialności za konfigurację aplikacyjną systemu SOWA SQL**, za którą odpowiada Administrator Systemu SOWA SQL; współpraca odbywa się jedynie w zakresie infrastruktury technicznej, jeśli jest to wymagane.

§ 6 Obowiązki Administratora Systemu Informatycznego SOWA SQL

Do obowiązków Administratora Systemu SOWA SQL należy:

1. **Przestrzeganie obowiązujących procedur operacyjnych oraz procedur bezpieczeństwa**, określonych w niniejszej Instrukcji i w pozostałych dokumentach wewnętrznych dotyczących bezpieczeństwa informacji.
2. **Zarządzanie aplikacyjną warstwą systemu SOWA SQL**, obejmujące konfigurację funkcji, modułów oraz ustawień systemowych zapewniających prawidłowe działanie systemu i bezpieczeństwo przetwarzanych danych osobowych.
3. **Zarządzanie użytkownikami systemu SOWA SQL**, w tym:
    - zakładanie kont,
    - modyfikacja uprawnień,
    - blokowanie lub usuwanie kont użytkowników,

    zgodnie z zaakceptowanymi wnioskami oraz obowiązującymi procedurami nadawania uprawnień.
4. **Nadzór nad aktualizacjami systemu SOWA SQL**, w tym współpraca z dostawcą oprogramowania oraz opiniowanie zasadności wdrażania aktualizacji, w porozumieniu z ASI w przypadku aktualizacji wymagających interwencji na poziomie infrastruktury informatycznej.
5. **Nadzór nad procesem wykonywania kopii zapasowych danych systemu SOWA SQL**, w tym okresowe potwierdzanie poprawności wykonywania kopii oraz weryfikacja kompletności danych, z uwzględnieniem zasad określonych przez dostawcę lub procedury wewnętrzne.
6. **Monitorowanie prawidłowego funkcjonowania systemu SOWA SQL**, zgłaszanie nieprawidłowości, awarii lub podejrzeń naruszenia bezpieczeństwa do ASI oraz IOD oraz współpraca przy ich usuwaniu w zakresie wynikającym z obowiązków Administratora Systemu.
7. **Prowadzenie czynności konserwacyjnych dotyczących warstwy aplikacyjnej systemu SOWA SQL**, w szczególności kontroli spójności danych, przeglądu konfiguracji oraz współpracy z Instruktorem w zakresie zagadnień merytorycznych związanych z pracą systemu.

8. **Współpraca z Administratorem Systemów Informatycznych oraz z Instruktorem**, w zakresie wynikającym z potrzeby utrzymania ciągłości działania systemu, w szczególności w obszarach wymagających wsparcia infrastrukturalnego lub merytorycznego.
9. **Zakres obowiązków Administratora Systemu Informatycznego SOWA SQL** obejmuje wyłącznie czynności związane z warstwą aplikacyjną systemu. Zadania związane z utrzymaniem infrastruktury technicznej, w tym systemów operacyjnych, sieci, domeny, sprzętu komputerowego oraz kopii zapasowych infrastruktury, realizowane są przez Administratora Systemów Informatycznych.

§ 7 Obowiązki użytkowników

1. Do obowiązków użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe, należy:
   a) **przestrzeganie zasad przetwarzania danych osobowych** obowiązujących w Bibliotece oraz wykonywanie czynności związanych z przetwarzaniem danych wyłącznie w zakresie wynikającym z powierzonych obowiązków i nadanego upoważnienia;
   b) **przestrzeganie procedur operacyjnych i procedur bezpieczeństwa**, określonych w niniejszej Instrukcji, Polityce Bezpieczeństwa oraz innych regulacjach wewnętrznych;
   c) **zapewnienie ochrony danych osobowych przed dostępem osób nieupoważnionych**, w szczególności poprzez stosowanie zasad bezpiecznego logowania, nieudostępnianie haseł oraz zabezpieczanie stanowiska pracy podczas nieobecności;
   d) **udostępnianie danych osobowych wyłącznie osobom posiadającym stosowne upoważnienie**, zgodnie z obowiązującymi przepisami i procedurami;
   e) **niezwłoczne zgłaszanie Inspektorowi Ochrony Danych**, a w razie potrzeby także przełożonemu lub Administratorowi Systemów Informatycznych, wszelkich incydentów, podejrzeń naruszenia bezpieczeństwa danych lub nieprawidłowości związanych z przetwarzaniem danych osobowych;
   f) **wykonywanie zaleceń i instrukcji Inspektora Ochrony Danych** dotyczących ochrony danych osobowych, w zakresie zgodnym z obowiązującymi przepisami prawa oraz zakresem powierzonych obowiązków;
   g) **przestrzeganie zasad korzystania z infrastruktury informatycznej**, w szczególności zakazu samowolnego podłączania urządzeń sieciowych, zakazu ingerowania w ustawienia sieci lub wprowadzania zmian mogących zakłócić jej działanie;
2. **W przypadku stwierdzenia nieautoryzowanego podłączenia urządzeń lub zakłóceń pracy sieci** użytkownik niezwłocznie informuje o tym fakcie Administratora Systemów Informatycznych. Administrator Systemów Informatycznych, w celu zapewnienia bezpieczeństwa infrastruktury i danych, **może tymczasowo odłączyć odpowiedni segment sieci** lub konto użytkownika do czasu wyjaśnienia sytuacji i usunięcia zagrożenia.

§ 8 NADAWANIE, ZMIANA I ODBIERANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH w systemach informatycznych

Zasady ogólne

1. Nadawanie, zmiana oraz odbieranie uprawnień do systemów informatycznych, w których przetwarzane są dane osobowe, odbywa się wyłącznie na podstawie wniosku złożonego przez bezpośredniego przełożonego użytkownika.
2. Upoważnienie do przetwarzania danych osobowych jest nadawane przez Administratora Danych Osobowych lub osobę przez ADO upoważnioną. Nadanie upoważnienia stanowi podstawę do rozpoczęcia procesu tworzenia konta w systemie informatycznym.
3. Dostęp systemowy (techniczny) przyznaje Administrator Systemów Informatycznych lub odpowiednio Administrator Systemu SOWA SQL w zakresie właściwym dla danego systemu, zgodnie z przyjętym zakresem obowiązków.
4. Użytkownik może przystąpić do pracy związanej z dostępem do danych osobowych wyłącznie po:
   a) podpisaniu upoważnienia do przetwarzania danych osobowych,
   b) złożeniu oświadczenia o zachowaniu poufności,
   c) odbyciu szkolenia wstępnego w zakresie ochrony danych osobowych i bezpieczeństwa informacji,
   d) odbyciu szkolenia stanowiskowego w zakresie obsługi systemów informatycznych, których będzie używał.

Nadawanie uprawnień

1. Wniosek o nadanie uprawnień składa bezpośredni przełożony pracownika, określając zakres uprawnień niezbędnych do wykonywania obowiązków służbowych.
2. Na podstawie zatwierdzonego wniosku, zgodnie z zakresem uprawnień określonych we wniosku:
   a) Administrator Systemów Informatycznych zakłada konto i nadaje uprawnienia w systemach infrastrukturalnych (Windows, domena, systemy operacyjne, sieć),
   b) Administrator Systemu SOWA SQL zakłada konto i nadaje uprawnienia w systemie SOWA SQL.
3. Identyfikator i zakres uprawnień użytkownika są rejestrowane:
   a) w ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzonej przez ADO,
   b) w ewidencji kont systemowych prowadzonej przez ASI lub Administratora Systemu Informatycznego SOWA SQL – w zależności od systemu.

4. Przy pierwszym logowaniu użytkownik jest zobowiązany do zmiany hasła zgodnie z zasadami bezpieczeństwa określonymi w Instrukcji.
5. Osoby niebędące pracownikami etatowymi (np. zleceniobiorcy, serwisanci, stażyści) mogą otrzymać wyłącznie dostęp czasowy, w zakresie niezbędnym do realizacji zadań, na okres wskazany we wniosku.

Zmiana uprawnień

1. Zmiana uprawnień jest dokonywana na pisemny wniosek przełożonego pracownika, w poniższych przypadkach:
   a) zmiana stanowiska lub zakresu obowiązków,
   b) awans,
   c) reorganizacja pracy,
   d) potrzeba rozszerzenia lub ograniczenia dostępu,
   e) inne uzasadnione potrzeby Biblioteki.
2. Zmiana uprawnień jest dokumentowana w ewidencji upoważnień i ewidencji kont systemowych.

Odbieranie / wyrejestrowanie uprawnień

1. Ustanie zatrudnienia, zakończenie współpracy, zmiana stanowiska lub długotrwała nieobecność powoduje konieczność niezwłocznego odebrania użytkownikowi dotychczasowych uprawnień do systemów informatycznych.
2. Odebranie uprawnień następuje:
   a) po zgłoszeniu przez przełożonego,
   b) na wniosek Działu Kadr po zakończeniu współpracy,
   c) na polecenie ADO lub IOD w przypadku incydentów bezpieczeństwa.
3. Wyrejestrowania dokonuje:
   a) Administrator Systemów Informatycznych – dla systemów infrastrukturalnych,
   b) Administrator Systemu SOWA SQL – dla systemu SOWA SQL.
4. Zmiana lub odbieranie uprawnień jest odnotowywane w ewidencjach, o których mowa w pkt 3 powyżej.

Zasady szczególne

1. Każdy użytkownik ponosi odpowiedzialność za wszystkie działania wykonane przez osobę posługującą się przydzielonym użytkownikowi identyfikatorem.
2. Zabrania się udostępniania identyfikatora lub hasła innym osobom oraz stosowania haseł łatwych do odgadnięcia.
3. Przekroczenie zakresu uprawnień stanowi naruszenie obowiązków pracowniczych i może być zakwalifikowane jako naruszenie bezpieczeństwa danych osobowych.

§ 9 Metody i środki uwierzytelniania

Identyfikator

1. Identyfikator użytkownika powinien składać się z ciągu znaków alfanumerycznych, zgodnie z zasadami ustalonymi przez Administratora Systemów Informatycznych.
2. Identyfikator użytkownika musi być unikalny i przypisany wyłącznie jednej osobie.
3. Identyfikator nie powinien zawierać informacji umożliwiających jednoznaczną identyfikację użytkownika przez osoby postronne (np. pełnego imienia i nazwiska), chyba że jest to konieczne ze względów organizacyjnych.

Hasło

1. Hasło musi być unikalnym ciągiem **co najmniej 12 znaków** i zawierać:

   - duże i małe litery,
   - cyfry,
   - znaki specjalne.

2. Hasło nie może być identyczne ani podobne do identyfikatora użytkownika oraz nie może zawierać danych łatwych do odgadnięcia (np. imię, nazwisko, data urodzenia, nazwy własne, numery telefonów).
3. Hasło powinno być łatwe do zapamiętania dla użytkownika, lecz trudne do odgadnięcia przez inne osoby.
4. System informatyczny powinien wymuszać **zmianę hasła nie rzadziej niż co 90 dni**. W uzasadnionych przypadkach Administrator Systemów Informatycznych może wymusić zmianę hasła w krótszym okresie (np. po incydencie bezpieczeństwa).
5. W przypadku systemów, które nie posiadają funkcji wymuszania zmiany hasła, użytkownik jest zobowiązany do **samodzielnej zmiany hasła co 90 dni**.
6. Zabrania się ponownego używania haseł używanych wcześniej.
7. Użytkownik nie może udostępniać identyfikatora i hasła innym osobom ani korzystać z danych logowania innego użytkownika.
8. Użytkownik jest odpowiedzialny za utrzymanie swojego hasła w poufności oraz jego właściwe zabezpieczenie.
9. Zabrania się przechowywania haseł w miejscach widocznych lub w formie niezaszyfrowanej (np. w dokumentach papierowych, plikach tekstowych, makrach, skryptach lub przeglądarce).
10. Podczas wpisywania hasła użytkownik powinien zabezpieczyć ekran i klawiaturę przed możliwością przeczytania hasła przez osoby trzecie.
11. W przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej, użytkownik jest zobowiązany do **niezwłocznej zmiany hasła** oraz zgłoszenia zdarzenia Administratorowi Systemów Informatycznych lub Inspektorowi Ochrony Danych.
12. Hasła zachowują status informacji poufnej również po wygaśnięciu.

13. Administrator Systemów Informatycznych jest odpowiedzialny za okresową weryfikację listy użytkowników oraz blokowanie lub usuwanie kont, które nie są już potrzebne.
14. Administrator Systemów Informatycznych powinien przeprowadzać **przegląd uprawnień nie rzadziej niż co 3 miesiące**. Każdy przegląd musi być udokumentowany.

Hasła Administratora Systemów Informatycznych

1. Hasła do kont administracyjnych (wysokich uprawnień) muszą być przechowywane w sposób zapewniający najwyższy poziom bezpieczeństwa.
2. Dostęp do haseł kont administracyjnych mogą posiadać wyłącznie:
    a) Administrator Danych Osobowych,
    b) Administrator Systemów Informatycznych.
3. Konta administracyjne mogą być wykorzystywane wyłącznie w sytuacjach uzasadnionych potrzebami technicznymi lub bezpieczeństwa.
4. Każde użycie konta administracyjnego powinno zostać odnotowane i udokumentowane.

§ 10 Procedura rozpoczęcia, zawieszenia oraz zakończenia pracy przez użytkowników systemu

Praca na stacjach roboczych

Rozpoczęcie pracy na stacji roboczej

1. Rozpoczęcie pracy następuje po uruchomieniu komputera i zalogowaniu się do systemu z wykorzystaniem indywidualnego identyfikatora i hasła użytkownika.
2. W pomieszczeniach, w których przetwarzane są dane osobowe, osoby postronne mogą przebywać wyłącznie za zgodą oraz pod nadzorem użytkownika lub osoby upoważnionej.
3. Na wszystkich komputerach, na których przetwarzane są dane osobowe, powinien być ustawiony **wygaszacz ekranu z funkcją blokady**, uruchamiający się po maksymalnie **10 minutach** bezczynności. Wznowienie pracy jest możliwe wyłącznie po podaniu hasła użytkownika.

Zawieszenie pracy (czasowe opuszczenie stanowiska)

1. Użytkownik opuszczając stanowisko pracy jest zobowiązany do:
    a) wylogowania się z systemu lub
    b) zastosowania blokady ekranu (np. kombinacja klawiszy).
2. Pozostawienie aktywnego i niezabezpieczonego stanowiska pracy jest niedopuszczalne.

3. Dokumenty papierowe zawierające dane osobowe muszą być zabezpieczone przed dostępem osób nieuprawnionych, w szczególności poprzez umieszczenie ich w zamykanych szafach lub szufladach.

Przetwarzanie danych w trakcie pracy

1. Przesyłanie danych osobowych pocztą elektroniczną powinno odbywać się wyłącznie w sposób zapewniający ich poufność, w szczególności poprzez szyfrowanie treści wiadomości lub stosowanie innych zatwierdzonych środków zabezpieczenia.
2. Użytkownik zobowiązany jest do prowadzenia pracy w sposób zapewniający integralność danych, w tym do wprowadzania danych do właściwych systemów i obszarów zgodnie z obowiązującymi procedurami

Zakończenie pracy

1. Po zakończeniu pracy użytkownik jest zobowiązany do:
   a) zapisania i zamknięcia przetwarzanych danych w systemie informatycznym,
   b) prawidłowego wylogowania się z systemu,
   c) zamknięcia wszystkich aplikacji i systemów,
   d) wyłączenia komputera, o ile nie stosuje się innych procedur technicznych Administratora Systemów Informatycznych.
2. Wszystkie dokumenty papierowe zawierające dane osobowe należy:
   a) zabezpieczyć w zamykanych na klucz szafach lub innym miejscu do tego przeznaczonym,
   b) niezwłocznie zniszczyć w niszczarce, jeżeli nie są już potrzebne do dalszego przetwarzania.
3. Jeżeli to możliwe, po zakończeniu pracy pomieszczenie, w którym przetwarzane są dane osobowe, powinno zostać zamknięte na klucz.

Praca na komputerach przenośnych

Szczegółowe zasady przetwarzania danych osobowych na komputerach przenośnych określa „Regulamin Przetwarzania Danych na Urządzeniach Przenośnych", stanowiący załącznik do niniejszej Instrukcji.

§ 11 Procedura tworzenia kopii zapasowych

Zasady ogólne

1. Kopie zapasowe danych oraz elementów systemów informatycznych są wykonywane w celu zapewnienia ciągłości działania Biblioteki oraz ochrony danych osobowych przed utratą, uszkodzeniem lub nieuprawnioną modyfikacją.
2. Kopie zapasowe systemów informatycznych, w tym systemu SOWA SQL, są wykonywane przez upoważnione podmioty zewnętrzne lub przez Administratora Systemów Informatycznych – zgodnie z zawartymi umowami oraz wewnętrznymi procedurami.
3. W przypadku wykonywania kopii zapasowych przez podmiot zewnętrzny:
   a) przetwarzanie danych osobowych odbywa się na podstawie **umowy powierzenia przetwarzania danych osobowych**,
   b) osoby wykonujące kopie muszą posiadać imienne upoważnienia do przetwarzania danych osobowych,
   c) podmiot zewnętrzny jest zobowiązany do stosowania środków bezpieczeństwa zgodnych z RODO i Krajowymi Ramami Interoperacyjności.
4. Kopie zapasowe muszą obejmować wszystkie istotne zbiory danych i konfiguracje niezbędne do odtworzenia działania systemów.

Tworzenie kopii zapasowych

1. Kopie zapasowe wykonywane są zgodnie z harmonogramem ustalonym przez Administratora Systemów Informatycznych lub przez podmiot zewnętrzny, zgodnie z umową.
2. W przypadku systemów pracujących w architekturze klient–serwer, kopie wykonywane są po stronie serwera lub środowiska, w którym hostowany jest system (np. serwery lokalne, środowisko chmurowe, infrastruktura dostawcy).
3. Proces tworzenia kopii obejmuje:
   a) dane systemowe,
   b) dane aplikacyjne,
   c) konfiguracje systemowe,
   d) inne elementy niezbędne do odtworzenia działania systemu.
4. Procedura wykonywania kopii zapasowych musi zapewniać:
   a) poufność danych,
   b) integralność danych,
   c) możliwość odtworzenia danych w przypadku awarii.

Przechowywanie kopii zapasowych

1. Kopie zapasowe są przechowywane w sposób zapewniający:
   a) ochronę przed dostępem osób nieuprawnionych,

b) ochronę przed utratą lub uszkodzeniem,
c) zachowanie integralności danych.

2. Kopie mogą być przechowywane:
a) na serwerach Biblioteki,
b) w infrastrukturze podmiotu zewnętrznego,
c) w lokalizacjach zapasowych,
zgodnie z przyjętą polityką bezpieczeństwa.
3. Liczba przechowywanych kopii zapasowych oraz okres przechowywania określane są w harmonogramie kopii zapasowych lub w umowie z podmiotem zewnętrznym.

Testowanie kopii zapasowych

1. W celu zapewnienia możliwości skutecznego odtworzenia danych, kopie zapasowe poddaje się testowemu odtworzeniu **co najmniej raz na 6 tygodni** lub zgodnie z harmonogramem określonym przez ASI lub podmiot zewnętrzny.
2. Test odtworzenia polega na:
a) próbnej rekonstrukcji danych lub konfiguracji systemu,
b) sprawdzeniu spójności i poprawności danych,
c) potwierdzeniu możliwości pełnego odtworzenia systemu.
3. Wyniki testów powinny być dokumentowane i archiwizowane.

Likwidacja nośników zawierających kopie zapasowe

1. Nośniki zawierające kopie zapasowe, które utraciły swoją przydatność, muszą zostać zniszczone lub oczyszczone w sposób uniemożliwiający odzyskanie danych.
2. W przypadku nośników jednorazowych (np. płyty DVD, pendrivy jednorazowe) likwidacja polega na fizycznym zniszczeniu nośnika.
3. Nośniki wielokrotnego użytku mogą być ponownie wykorzystywane po zastosowaniu procedur trwałego usunięcia danych (np. nadpisanie wielokrotne, demagnetyzacja, procedury wskazane przez producenta lub podmiot zewnętrzny).
4. Uszkodzone nośniki wielokrotnego użytku należy zniszczyć fizycznie, np. w niszczarce specjalistycznej lub poprzez usługę utylizacji świadczoną przez podmiot zewnętrzny.

§ 12 Procedura postępowania na wypadek wystąpienia awarii

Postępowanie w przypadku awarii jednostkowej

Postanowienia ogólne

Awarię rozumie się jako stan niesprawności systemu informatycznego lub elementu infrastruktury IT, powodujący jego nieprawidłowe działanie lub całkowite unieruchomienie.

1. Wszelkie awarie należy zgłaszać poprzez:

a) zgłoszenie e-mail na adres: awaria@bppragapd.pl,
b) lub telefonicznie – zgodnie z listą kontaktów wewnętrznych.

2. Zgłoszenie awarii powinno zawierać:
   a) rodzaj awarii,
   b) nazwę filii/oddziału Biblioteki,
   c) opis problemu,
   d) datę i godzinę wystąpienia,
   e) osobę zgłaszającą.
   a) Obsługa czytelnika w czasie awarii jest realizowana zgodnie z procedurami opisanymi w dalszej części rozdziału.

Postępowanie w przypadku awarii jednostkowej

(dotyczy jednego stanowiska, użytkownika lub komputera zgodnie z definicją w § 3 Instrukcji)

1. **Zgłoszenie awarii jednostkowej**
   a) Kierownik filii lub osoba zastępująca kierownika zgłasza awarię:
      - na adres **awaria@bppragapd.pl** lub
      - telefonicznie do Działu Komputeryzacji i Edukacji Informatycznej (ASI).
   b) W przypadku awarii w systemie SOWA SQL zgłoszenie kierowane jest dodatkowo do:
      - Administratora Systemu SOWA SQL lub
      - Instruktora.
2. **Postępowanie**
   a) Dział Komputeryzacji i Edukacji Informatycznej diagnozuje i usuwa awarię w zakresie infrastruktury IT.
   b) Administrator Systemu SOWA SQL diagnozuje problemy dotyczące systemu SOWA SQL.
   c) Obsługa czytelnika powinna być możliwa na drugim, zdublowanym stanowisku, o ile takie funkcjonuje.

Postępowanie w przypadku awarii zwykłej (operacyjnej)

(dotyczy wielu stanowisk w jednej filii lub ograniczonej funkcjonalności systemów zgodnie z definicją w § 3 Instrukcji)

Zgłoszenie awarii

1. Kierownik filii lub osoba zastępująca kierownika zgłasza awarię na adres: awaria@bppragapd.pl lub telefonicznie do ASI.
2. W przypadku awarii systemu SOWA SQL zgłoszenie trafia również do Administratora Systemu SOWA SQL / Instruktora.
3. W przypadku awarii sieci lub internetu zgłoszenie kierowane jest do ASI.

Postępowanie

1. ASI diagnozuje awarie infrastrukturalne (internet, sieć, sprzęt).
2. Administrator Systemu SOWA SQL diagnozuje i usuwa awarie aplikacyjne.

Zasady obsługi w czasie awarii zwykłej:

1. Kierownik filii umieszcza informację o awarii w widocznym miejscu przy wejściu.
2. ASI umieszcza informację o awarii na stronie WWW i intranecie.
3. Zwroty i wypożyczenia książek są wstrzymane (w wyjątkowych sytuacjach kierownik placówki podejmuje decyzję co do obsługi czytelnika)
4. Zapisy nowych czytelników są wstrzymane.
5. W czasie awarii wydłuża się terminy zwrotu (prolongata) za czas, w którym system nie działał.

Postępowanie w przypadku awarii krytycznej

(paraliżującej pracę systemów w co najmniej jednej lokalizacji zgodnie z definicją *w § 3 Instrukcji)*

Zgłoszenie awarii

Kierownik filii zgłasza awarię zgodnie z procedurą na adres: awaria@bppragapd.pl lub telefonicznie do ASI.

Postępowanie techniczne

1. ASI niezwłocznie ustala przyczynę awarii dotyczącej infrastruktury IT.
2. W razie potrzeby:
   - kontaktuje się z dostawcą Internetu,
   - zgłasza problem do firmy serwisowej.
3. W przypadku awarii systemu SOWA SQL:
   - Administrator Systemu SOWA SQL ustala przyczynę i w razie potrzeby zgłasza problem firmie **SOKRATES-Software**.
   - ASI informuje **Inspektora Ochrony Danych** o awarii, jeśli może ona prowadzić do naruszenia ochrony danych osobowych.

Obsługa czytelnika w czasie awarii krytycznej

Obsługa czytelnika odbywa się zgodnie z zasadami określonymi dla awarii zwykłej.

Zalecenia dalszego postępowania

- W razie przedłużającej się awarii (zwykłej lub krytycznej) powyżej 4 godzin, kierownik filii konsultuje się z Instruktorem w celu ustalenia zasad organizacji pracy. Po ustaniu awarii krytycznej **ASI sporządza pisemny raport** i przekazuje go Dyrektorowi Biblioteki zgodnie z „Polityką zarządzania ryzykiem".
- Po ustaniu awarii zwykłej lub jednostkowej kierownik filii sporządza raport i przekazuje go pracownikowi ds. kontroli zarządczej. Jeżeli stwierdzono naruszenie ochrony danych osobowych, ASI w porozumieniu z IOD prowadzą postępowanie zgodnie z Instrukcją Bezpieczeństwa Informacji oraz Instrukcją Przetwarzania Danych Osobowych.

§ 12 Przechowywanie elektronicznych nośników informacji z danymi osobowymi

Zasady ogólne przechowywania danych

1. Dane osobowe w postaci elektronicznej przechowywane są wyłącznie na serwerach oraz w systemach informatycznych wykorzystywanych przez Administratora Danych lub podmioty przetwarzające działające na podstawie umowy powierzenia przetwarzania danych osobowych.
2. Dane osobowe, które są czasowo przetwarzane na stacjach roboczych lub komputerach przenośnych, powinny być niezwłocznie zapisane w systemach informatycznych lub na serwerach przeznaczonych do ich przetwarzania, zgodnie z organizacją pracy i obowiązującymi procedurami.

Zewnętrzne nośniki danych

1. Zabrania się przechowywania lub przetwarzania danych osobowych na zewnętrznych elektronicznych nośnikach informacji (np. pendrive'ach, zewnętrznych dyskach, kartach pamięci, płytach DVD), chyba że jest to niezbędne do realizacji zadań służbowych i zostało wyraźnie dopuszczone przez Administratora Danych w odrębnych regulacjach.
2. W przypadku potrzeby skorzystania z nośników zgodnie z pkt. 1, nośniki muszą być:
   a) szyfrowane zgodnie z procedurami bezpieczeństwa,
   b) zabezpieczone przed dostępem osób nieupoważnionych,
   c) ewidencjonowane przez Administratora Systemów Informatycznych lub wyznaczoną osobę.

Przechowywanie danych systemu SOWA SQL

1. Zbiory danych Systemu Bibliotecznego **SOWA SQL** przechowywane są na serwerach hostingowych zewnętrznego podmiotu **SOKRATES-Software**, zgodnie z zawartą

umową oraz zasadami bezpieczeństwa określonymi przez dostawcę systemu i Administratora Danych.

2. SOKRATES-Software jako podmiot przetwarzający jest zobowiązana do stosowania środków bezpieczeństwa zgodnych z RODO i innymi przepisami dotyczącymi ochrony danych osobowych.

Bezpieczeństwo przechowywania danych

1. Elektroniczne nośniki danych oraz urządzenia wykorzystywane do przetwarzania danych osobowych muszą być zabezpieczone przed dostępem osób nieupoważnionych.
2. Przechowywanie danych osobowych w formie lokalnej (np. pliki eksportowe, raporty) jest dopuszczalne wyłącznie w przypadkach uzasadnionych, a dane te muszą być niezwłocznie przeniesione do systemu informatycznego i usunięte ze stacji roboczej po ich wykorzystaniu.

§ 13 ZABEZPIECZENIE SYSTEMÓW INFORMATYCZNYCH PRZED ZŁOŚLIWYM OPROGRAMOWANIEM.

Zasady ogólne

1. Administrator Systemów Informatycznych zapewnia stosowanie narzędzi i mechanizmów chroniących systemy informatyczne Biblioteki przed złośliwym oprogramowaniem, próbami nieuprawnionego dostępu oraz innymi zagrożeniami pojawiającymi się w sieci.

2. Ochrona obejmuje wszystkie elementy infrastruktury informatycznej, w tym serwery, stacje robocze, komputery przenośne, urządzenia sieciowe oraz systemy aplikacyjne.

Ochrona antywirusowa i antymalware

1. Na wszystkich urządzeniach, na których przetwarzane są dane osobowe, musi być zainstalowane oprogramowanie antywirusowe / antymalware z funkcją:
    1. ochrony w czasie rzeczywistym,
    2. automatycznej aktualizacji,
    3. automatycznego skanowania,
    4. wykrywania zagrożeń behawioralnych.
2. Administrator Systemów Informatycznych zapewnia automatyczną aktualizację:
    a) definicji zagrożeń,
    b) oprogramowania zabezpieczającego,
    c) silnika skanującego.

3. Pełne skanowanie systemów może być uruchamiane automatycznie według ustalonego harmonogramu lub ręcznie w przypadkach szczególnych (incydenty, podejrzenia infekcji).

Zapobieganie zagrożeniom ze strony sieci i Internetu

1. Sieć wewnętrzna Biblioteki jest zabezpieczona centralnym urządzeniem z funkcjami firewall oraz filtrowania ruchu sieciowego.
2. Administrator Systemów Informatycznych konfiguruje zasady filtrowania i ochrony sieci, w tym:
   a) blokowanie ruchu nieautoryzowanego,
   b) kontrolę dostępu do usług sieciowych,
   c) monitorowanie anomalii w ruchu sieciowym,
   d) zabezpieczenia przed atakami typu ransomware, phishing, exploit.
3. Dostęp do Internetu jest możliwy wyłącznie za pośrednictwem urządzeń i połączeń kontrolowanych przez Bibliotekę.

Postępowanie z nośnikami zewnętrznymi

1. Korzystanie z przenośnych nośników danych (pendrive, dyski zewnętrzne) jest dopuszczalne jedynie w celach służbowych i wyłącznie na urządzeniach Biblioteki lub jej partnerów.
2. Każdy zewnętrzny nośnik danych musi zostać automatycznie lub ręcznie sprawdzony przez oprogramowanie antywirusowe przed otwarciem lub skopiowaniem danych.
3. W przypadku wykrycia zagrożenia, użytkownik jest zobowiązany przerwać pracę z nośnikiem i niezwłocznie powiadomić Administratora Systemów Informatycznych.

Rola użytkowników

1. Użytkownik jest zobowiązany:
   a) zgłaszać wszelkie komunikaty o zagrożeniach lub podejrzanych działaniach systemu,
   b) nie otwierać podejrzanych załączników i linków,
   c) korzystać jedynie z zatwierdzonych aplikacji i stron internetowych.
2. Zabrania się instalowania jakiegokolwiek oprogramowania bez zgody Administratora Systemów Informatycznych.

Działania administratora systemów

1. Administrator Systemów Informatycznych:
   a) monitoruje działanie oprogramowania zabezpieczającego,
   b) analizuje zgłoszenia użytkowników,
   c) podejmuje działania zapobiegawcze i naprawcze,
   d) usuwa wykryte zagrożenia,
   e) w razie potrzeby kontaktuje się z dostawcami usług i oprogramowania.

2. W przypadku podejrzenia naruszenia ochrony danych osobowych Administrator Systemów Informatycznych niezwłocznie informuje Inspektora Ochrony Danych.

§ 14 REJESTROWANIE OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

Rejestrowanie wprowadzania i modyfikacji danych

1. Systemy informatyczne wykorzystywane do przetwarzania danych osobowych muszą umożliwiać automatyczne rejestrowanie (logowanie) operacji wykonywanych na danych, w szczególności:
   a) pierwszego wprowadzenia danych,
   b) modyfikacji danych,
   c) usunięcia danych,
   d) osoby (identyfikatora użytkownika) wykonującej czynność,
   e) daty i czasu wykonania operacji.

2. Logi operacji muszą być przechowywane w sposób uniemożliwiający ich modyfikację przez użytkowników nieuprawnionych oraz dostępne dla Administratora Systemów Informatycznych, Administratora Danych oraz Inspektora Ochrony Danych — w zakresie niezbędnym do realizacji obowiązków.

Rejestrowanie udostępnień danych

Systemy, w których dane osobowe są udostępniane podmiotom zewnętrznym lub odbiorcom danych, powinny umożliwiać odnotowanie informacji:
a) komu dane zostały udostępnione,
b) daty i czasu udostępnienia,
c) zakresu udostępnionych danych,
d) podstawy prawnej udostępnienia,
chyba że dane pochodzą z jawnego zbioru danych osobowych.

Rejestrowanie sprzeciwów i ograniczeń w przetwarzaniu

1. System informatyczny powinien umożliwiać odnotowanie każdego przypadku zgłoszenia:
   a) sprzeciwu wobec przetwarzania danych osobowych (art. 21 RODO),
   b) żądania ograniczenia przetwarzania (art. 18 RODO).

2. Informacja o sprzeciwie lub ograniczeniu musi być powiązana z kontem użytkownika lub identyfikatorem rekordu i widoczna przy każdej operacji przetwarzania.

Zakaz kodowania znaczeń w identyfikatorach

Zabrania się nadawania ukrytych znaczeń elementom numeracji, oznaczeń lub identyfikatorów stosowanych w systemach ewidencyjnych, jeżeli mogłyby one prowadzić do ujawnienia dodatkowych informacji o osobie (np. wieku, płci, statusu, lokalizacji), co mogłoby naruszać zasady minimalizacji danych i poufności.

Zasady przechowywania logów

1. Logi systemowe związane z operacjami przetwarzania danych osobowych muszą być przechowywane przez okres zgodny z polityką bezpieczeństwa Biblioteki oraz wymaganiami wynikającymi z RODO i polityki zarządzania ryzykiem.

2. Dostęp do logów mają wyłącznie osoby upoważnione:

    - Administrator Systemów Informatycznych,
    - Administrator Danych Osobowych (lub osoba przez niego wyznaczona),
    - Inspektor Ochrony Danych — w zakresie niezbędnym do realizacji nadzoru.

§ 15 KONSERWACJA, PRZEGLĄDY I UTRZYMANIE SYSTEMÓW INFORMATYCZNYCH ORAZ NOŚNIKÓW DANYCH

Zakres i odpowiedzialność

1. Konserwację, serwis oraz bieżące utrzymanie systemów informatycznych, urządzeń i nośników danych wykonuje **Administrator Systemów Informatycznych (ASI)** lub osoby przez ASI upoważnione.

2. Konserwacja może być wykonywana również przez podmioty zewnętrzne, z którymi zawarto umowy serwisowe lub umowy powierzenia przetwarzania danych osobowych — zgodnie z zakresem tych umów.

3. Inspektor Ochrony Danych (IOD) nie wykonuje czynności technicznych, natomiast może przeprowadzać **kontrolę zgodności** procesu konserwacji z przepisami o ochronie danych osobowych.

Konserwacja systemów informatycznych

1. Konserwacja obejmuje w szczególności:
   a) aktualizację oprogramowania systemowego i aplikacyjnego,
   b) instalację poprawek bezpieczeństwa,
   c) kontrolę poprawności działania oprogramowania antywirusowego i zabezpieczeń sieciowych,
   d) usuwanie usterek sprzętowych i programowych,

e) kontrolę integralności danych i systemów,
f) przeglądy logów i alertów bezpieczeństwa,
g) modernizację sprzętu i oprogramowania, jeśli jest to wymagane.

2. Wszystkie prace konserwacyjne powinny być wykonywane w sposób zapewniający:

   a) ochronę integralności danych,
   b) nienaruszalność zbiorów danych osobowych,
   c) ciągłość działania systemów,
   d) minimalizację ryzyka utraty danych.

Konserwacja nośników informacji

1. Nośniki danych, na których znajdują się dane osobowe (dyski, pamięci masowe, zasoby sieciowe), podlegają okresowym przeglądom w celu:

   a) wykrycia usterek,
   b) zapewnienia poprawnej pracy,
   c) zapobiegania uszkodzeniom mogącym spowodować utratę danych.

2. Nośniki uszkodzone, zdegradowane lub wycofane z użycia są likwidowane zgodnie z rozdziałem dotyczącym usuwania nośników (niszczenie lub trwałe kasowanie danych).

Przeglądy poprawności danych

1. Przeglądy poprawności i integralności danych zawartych w systemach wykonuje:

   a) Administrator Systemów Informatycznych (w zakresie technicznym),
   b) Administrator Systemu SOWA SQL (w zakresie danych bibliotecznych),
   c) podmiot zewnętrzny obsługujący system — w ramach umowy serwisowej.

2. Inspektor Ochrony Danych może kontrolować realizację przeglądów pod kątem zgodności z RODO, ale **nie wykonuje technicznych prac na danych**.

3. W przypadku wykrycia błędów w danych:

   a) Administrator Systemu SOWA SQL lub osoba odpowiedzialna za dany system podejmuje działania naprawcze,
   b) ASI podejmuje działania techniczne (jeśli błąd dotyczy infrastruktury),
   c) informuje się osoby odpowiedzialne za właściwy moduł systemu.

Dokumentowanie prac konserwacyjnych

1. Wszystkie prace konserwacyjne, istotne zmiany konfiguracji oraz interwencje techniczne powinny być dokumentowane przez ASI lub podmiot zewnętrzny, który je wykonuje.

2. Dokumentacja powinna obejmować w szczególności:

- datę i zakres wykonanych prac,
- osobę lub firmę wykonującą,
- opis problemu (jeżeli konserwacja była wynikiem awarii),
- informację o wpływie na przetwarzanie danych osobowych (jeśli miało to miejsce).

§ 16 Serwis i naprawy urządzeń komputerowych oraz postępowanie z danymi osobowymi podczas serwisu urządzeń komputerowych

Zasady ogólne

1. Wszelkie naprawy, modernizacje oraz inne prace techniczne dotyczące urządzeń komputerowych lub systemów informatycznych wykorzystywanych do przetwarzania danych osobowych odbywają się **pod nadzorem Administratora Systemów Informatycznych (ASI)** lub osoby przez niego upoważnionej.
2. Celem nadzoru jest zapewnienie bezpieczeństwa danych osobowych oraz zapobieżenie ich przypadkowemu ujawnieniu, utracie lub nieuprawnionemu dostępowi.
3. Każda naprawa urządzeń komputerowych lub modyfikacja systemu informatycznego musi być odnotowana w dokumentacji serwisowej lub rejestrze czynności technicznych.

Naprawy wykonywane przez pracowników Biblioteki

1. Naprawy wykonywane przez ASI lub pracowników Biblioteki odbywają się w sposób zapewniający:
   a) ochronę integralności danych,
   b) brak możliwości ich utraty lub nieuprawnionego ujawnienia,
   c) minimalizację przerw w działaniu systemów.
2. W przypadku konieczności wymiany lub naprawy nośnika danych (np. dysku twardego, pamięci masowej), ASI zobowiązany jest do:
   a) wykonania kopii zapasowej danych,
   b) bezpiecznego usunięcia danych z uszkodzonego nośnika,
   c) potwierdzenia faktu usunięcia lub zniszczenia w dokumentacji.

Naprawy wykonywane przez podmioty zewnętrzne

1. W przypadku konieczności przekazania sprzętu do zewnętrznego serwisu:
   a) sprzęt przekazywany jest **po uprzednim trwałym usunięciu wszystkich danych osobowych**,
   b) jeśli trwałe usunięcie danych nie jest możliwe, przekazanie następuje **po podpisaniu umowy powierzenia przetwarzania danych osobowych** zgodnie z art. 28 RODO,
   c) z przekazania sprzętu sporządza się **protokół przekazania**, zawierający m.in. datę, zakres naprawy i dane serwisu.

2. Naprawy przez podmioty zewnętrzne, o ile to możliwe, wykonuje się **na terenie Biblioteki**, w obecności ASI lub osoby przez niego wyznaczonej.

Postępowanie z uszkodzonymi nośnikami danych

1. Nośniki danych (dyski, płyty, pamięci) uszkodzone w sposób uniemożliwiający ich odczyt lub skuteczne usunięcie danych podlegają **fizycznemu zniszczeniu** w sposób trwały, uniemożliwiający odzyskanie informacji.
2. Fizyczne zniszczenie może obejmować m.in.
   a) użycie specjalnej niszczarki do nośników danych,
   b) demagnetyzację,
   c) zniszczenie mechaniczne (np. rozdrobnienie).
3. Z każdego zniszczenia nośnika należy sporządzić **protokół zniszczenia**, potwierdzony przez ASI lub osobę upoważnioną.

Odpowiedzialność i kontrola

1. Za prawidłowe przeprowadzenie napraw oraz nadzór nad bezpieczeństwem danych osobowych odpowiada Administrator Systemów Informatycznych.
2. Inspektor Ochrony Danych może kontrolować poprawność realizacji napraw w zakresie zgodności z zasadami ochrony danych osobowych, bez udziału w pracach technicznych.

§ 17 Wymagania dotyczące sprzętu i oprogramowania

Licencjonowanie i legalność oprogramowania

1. Na wszystkich urządzeniach wykorzystywanych do przetwarzania danych osobowych mogą być instalowane wyłącznie programy posiadające ważne licencje lub legalne uprawnienia do użytkowania.
2. Oprogramowanie może być instalowane tylko po uzyskaniu zgody Administratora Systemów Informatycznych (ASI). Za nieautoryzowane uznaje się w szczególności:
   a) oprogramowanie Freeware, Shareware lub trial,
   b) aplikacje pobrane z Internetu bez weryfikacji,
   c) prywatne oprogramowanie użytkowników,
   o ile nie zostały zaakceptowane i dopuszczone do użycia przez ASI.
3. Zabrania się instalowania jakiegokolwiek oprogramowania na sprzęcie Biblioteki bez zgody ASI, niezależnie od jego rodzaju, ceny czy pochodzenia.

Wymagania dotyczące instalacji oprogramowania

1. Przed instalacją nowego oprogramowania ASI lub osoba przez niego upoważniona dokonuje oceny:
   a) wpływu na bezpieczeństwo systemów,
   b) wymagań sprzętowych i środowiskowych,
   c) zgodności z architekturą systemów w Bibliotece,
   d) wpływu na przetwarzanie danych osobowych.

2. Wdrażanie nowego oprogramowania lub aktualizacji odbywa się zgodnie z procedurą zarządzania zmianą, obejmującą:
   a) testy w wydzielonym środowisku (jeśli jest dostępne),
   b) dokumentację przeprowadzonych testów,
   c) akceptację ASI,
   d) bezpieczne wdrożenie do środowiska produkcyjnego.

Wymagania dotyczące sprzętu komputerowego

Urządzenia informatyczne wykorzystywane do przetwarzania danych osobowych muszą być zasilane z sieci energetycznej zabezpieczonej przed zakłóceniami, zgodnie z wymaganiami producenta sprzętu.

1. Serwery oraz kluczowe urządzenia sieciowe muszą być chronione zasilaniem awaryjnym (UPS) o parametrach umożliwiających:
   a) podtrzymanie pracy przez minimum 15 minut,
   b) bezpieczne zamknięcie systemów i zapis danych w przypadku dłuższego zaniku zasilania.

2. Sprzęt wykorzystywany do pracy z danymi osobowymi musi być regularnie aktualizowany, serwisowany oraz objęty wsparciem technicznym.

Zarządzanie wersjami i utrzymaniem oprogramowania

1. ASI jest odpowiedzialny za zapewnienie aktualności oprogramowania, w tym:
   a) systemów operacyjnych,
   b) aplikacji użytkowych,
   c) komponentów bezpieczeństwa (np. antywirus, firewall).
2. Przestarzałe wersje oprogramowania mogą być przechowywane jedynie wtedy, gdy jest to niezbędne do zapewnienia ciągłości działania lub celów archiwizacyjnych, a ich przechowywanie nie stwarza ryzyka dla bezpieczeństwa danych.

Monitorowanie i zabezpieczenia systemowe

1. Systemy informatyczne muszą umożliwiać rejestrowanie błędów, alertów oraz zdarzeń związanych z przetwarzaniem danych osobowych. Logi muszą być zabezpieczone przed usunięciem lub modyfikacją.

2. Informacje zawarte w dziennikach zdarzeń podlegają ochronie przed nieautoryzowanym dostępem oraz analizie przez ASI w zakresie bezpieczeństwa i niezawodności systemów.

3. ASI zobowiązany jest zapewnić, aby na urządzeniach informatycznych:
   a) porty, usługi i funkcje nieużywane były dezaktywowane,
   b) zbędne komponenty systemowe były usuwane lub blokowane,
   c) konfiguracja systemów minimalizowała ryzyko wystąpienia incydentów bezpieczeństwa.

§ 18 Badanie podatności i cykliczna ocena bezpieczeństwa systemów IT

Cel i zakres

1. Celem badań podatności systemów IT jest identyfikacja słabych punktów infrastruktury oraz aplikacji wykorzystywanych przez Bibliotekę, a następnie wdrożenie działań podnoszących poziom bezpieczeństwa przetwarzania danych osobowych i zapewniających ciągłość działania systemów.

2. Harmonogram cyklicznego badania podatności systemów IT stanowi Załącznik nr 2 do niniejszej Instrukcji. Terminy mogą ulegać zmianie z przyczyn organizacyjnych lub technicznych.

Zakres badań

1. Testy infrastruktury IT

Badania obejmują w szczególności:

a) Weryfikację aktualności systemów operacyjnych i oprogramowania (serwery, stacje robocze, urządzenia sieciowe).

b) Kontrolę konfiguracji usług sieciowych pod kątem:

- zbędnych/usuniętych usług,
- nieprawidłowej konfiguracji,
- narażenia na podatności.

c) Sprawdzenie stosowanych mechanizmów hasłowych i uwierzytelniania.

d) Weryfikację znanych podatności publikowanych przez producentów oraz w źródłach bezpieczeństwa (np. CVE).

e) Analizę innych zidentyfikowanych słabości mogących stanowić zagrożenie dla systemów Biblioteki.

2. Testy bezpieczeństwa aplikacji

Testy obejmują:

a) Mechanizmy uwierzytelniania i autoryzacji użytkowników.

b) Zarządzanie kontami i uprawnieniami.

c) Obsługę błędów, wyjątków i walidację danych wejściowych/wyjściowych.

d) Zasady działania funkcji administracyjnych systemów.

e) Pozostałe podatności wykryte podczas przeprowadzanych testów.

3. Przegląd dokumentacji bezpieczeństwa

Raz w roku dokonuje się przeglądu i aktualizacji:

a) Instrukcji Zarządzania Systemami Informatycznymi,
b) Polityki Bezpieczeństwa Informacji,
c) dokumentacji uzupełniającej związanej z ochroną danych osobowych.

Etapy badania

Badanie wykonywane jest corocznie i obejmuje następujące etapy:

a) Przeprowadzenie testów bezpieczeństwa.

b) Opracowanie raportu z testów.

c) Przygotowanie propozycji działań korygujących i zapobiegawczych.

d) Wdrożenie zatwierdzonych działań korygujących przez Administratora Systemów Informatycznych lub podmioty zewnętrzne (jeżeli dotyczy).

§ 19 Postanowienia końcowe

Zakres stosowania

W sprawach nieuregulowanych niniejszą Instrukcją stosuje się:

a) dokumentację techniczną urządzeń i oprogramowania,
b) Politykę Bezpieczeństwa Informacji,
c) obowiązujące przepisy prawa dotyczące ochrony danych osobowych i bezpieczeństwa informacji,
d) Krajowe Ramy Interoperacyjności,

Obowiązek zapoznania się z Instrukcją

1. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zapoznania się z niniejszą Instrukcją przed dopuszczeniem do pracy związanej z dostępem do danych oraz podpisania oświadczenia potwierdzającego znajomość jej zasad.

2. Oświadczenia przechowywane są w dokumentacji kadrowej lub w innym miejscu wskazanym przez Administratora Danych Osobowych.

Odpowiedzialność za naruszenia

1. Niedostosowanie się do zasad i procedur określonych w niniejszej Instrukcji przez pracowników może zostać potraktowane jako naruszenie obowiązków pracowniczych, z konsekwencjami przewidzianymi w obowiązujących przepisach prawa, w tym Kodeksie pracy.

2. Naruszenia dotyczące ochrony danych osobowych podlegają również procedurom zgłaszania incydentów bezpieczeństwa oraz postępowaniom określonym w Polityce Bezpieczeństwa Informacji.

Aktualizacja Instrukcji

1. Instrukcja podlega okresowemu przeglądowi, nie rzadziej niż raz na 12 miesięcy, a także każdorazowo po istotnych zmianach technologicznych lub organizacyjnych wpływających na sposób przetwarzania danych osobowych.

2. Za aktualizację Instrukcji odpowiada Administrator Danych we współpracy z Administratorem Systemów Informatycznych oraz Inspektorem Ochrony Danych.

Spis załączników

1. Załącznik nr 1 - Harmonogram cyklicznego badania podatności systemów IT
2. Załącznik nr 2 – Wykaz obiektów, w których przetwarzane są dane osobowe
3. Załącznik nr 3 – Wytyczne przetwarzania danych osobowych poza Biblioteką Publiczną im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy

DYREKTOR BIBLIOTEKI PUBLICZNEJ
im. Zygmunta Jana Rumla
w Dzielnicy Praga-Południe m.st. Warszawy
Iwona Kaczorowska

Załącznik nr 1 do *Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy*

HARMONOGRAM CYKLICZNEGO BADANIA PODATNOŚCI SYSTEMÓW IT													
Lp.	Nazwa zadania	Miesiąc roku											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Testy infrastruktury IT												
2	Testy bezpieczeństwa aplikacji												
3	Przegląd polityki bezpieczeństwa												

Legenda:

Testy *(nr tygodnia)*

Przygotowanie raportu z testów *(nr tygodnia)*

Propozycje działań korygujących *(nr tygodnia)*

Wprowadzenie działań korygujących *(nr tygodnia)*

Załącznik nr 2

Wykaz obiektów, gdzie przetwarzane są dane osobowe:

1. Biblioteka dla Dzieci i Młodzieży Nr 2 – ul. J. Meissnera 5, 03-982 Warszawa
2. Biblioteka dla Dzieci i Młodzieży Nr 16 – ul. Walewska 7a, 04-022 Warszawa
3. Biblioteka dla Dzieci i Młodzieży Nr 34 – ul. Jana Nowaka Jeziorańskiego 24, 03-982 Warszawa
4. Biblioteka dla Dzieci i Młodzieży Nr 42 – ul. Biskupia 50, 04-216 Warszawa
5. Biblioteka dla Dzieci i Młodzieży Nr 45 – ul. Meksykańska 3, 03-949 Warszawa
6. Biblioteka dla Dzieci i Młodzieży Nr 47 – ul. Paca 46, 04-386 Warszawa
7. Biblioteka dla Dzieci i Młodzieży Nr 55 – ul. Egipska 7, 00-999 Warszawa
8. Biblioteka dla Dzieci i Młodzieży Nr 67 – ul. Awionetki RWD 1, 03-982 Warszawa
9. Wypożyczalnia dla Dorosłych i Młodzieży Nr 3 – ul. Waszyngtona 2b, 03-910 Warszawa
10. Wypożyczalnia dla Dorosłych i Młodzieży Nr 18 – ul. Grochowska 118, 04-301 Warszawa
11. Wypożyczalnia dla Dorosłych i Młodzieży Nr 19 – ul, Meissnera 5, 03-982 Warszawa
12. Wypożyczalnia dla Dorosłych i Młodzieży Nr 24 – ul. Grochowska 279, 03-844 Warszawa.
13. Wypożyczalnia dla Dorosłych i Młodzieży Nr 40 – ul. Paca 46, 04-386 Warszawa
14. Wypożyczalnia dla Dorosłych i Młodzieży Nr 44 – ul. Jana Nowaka Jeziorańskiego 24, 03-982 Warszawa
15. Wypożyczalnia dla Dorosłych i Młodzieży Nr 62 – ul. Egipska 7, 00-999 Warszawa
16. Wypożyczalnia dla Dorosłych i Młodzieży Nr 66 – ul. Angorska 14, 03-913 Warszawa
17. Wypożyczalnia dla Dorosłych i Młodzieży Nr 78 – ul. Majdańska 5, 04-088 Warszawa
18. Wypożyczalnia dla Dorosłych i Młodzieży Nr 89 – ul. Grochowska 202, 04-357 Warszawa
19. Wypożyczalnia dla Dorosłych i Młodzieży Nr 90 – ul. Rozłucka 11a, 04-022 Warszawa
20. Wypożyczalnia dla Dorosłych i Młodzieży Nr 92 – ul. Biskupia 50, 04-216 Warszawa
21. Wypożyczalnia dla Dorosłych i Młodzieży Nr 94 – ul. Meksykańska 3, 03-949 Warszawa
22. Wypożyczalnia dla Dorosłych i Młodzieży Nr 100 – ul. Zwycięzców 46, 03-938 Warszawa
23. Wypożyczalnia dla Dorosłych i Młodzieży Nr 110 –ul. Awionetki RWD 1, 03-982 Warszawa
24. Wypożyczalnia Zbiorów Obcojęzycznych „Biblioteka Wielokulturowa" – ul. Jana Nowaka Jeziorańskiego 24, 03-982 Warszawa

25. Wypożyczalnia Książki Mówionej i Multimediów – ul. Meissnera 5, 03-982 Warszawa
26. Czytelnia Naukowa Nr V –ul. Meissnera 5, 03-982 Warszawa
27. Punkt Biblioteczny „Grochoteka" – ul. Grochowska 297, 03-844 Warszawa
28. Dział IT – ul. Meissnera 5, 03-982 Warszaw

Załącznik nr 3 do *Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy*

Wytyczne przetwarzania danych osobowych poza Biblioteką Publiczną im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy

Spis treści

Rozdział 1. Cel

Niniejsze wytyczne regulują zasady przetwarzania danych określone w Polityce Bezpieczeństwa Informacji (PBI) Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy, której celem jest określenie postępowania osób upoważnionych do przetwarzania danych osobowych, dokonywanego poza obiektami (obszarami przetwarzania) Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy:

1. w formie tradycyjnej (dokumenty papierowe),
2. w formie elektronicznej, tj. na urządzeniach stacjonarnych, mobilnych i nośnikach informacji:
   a. służbowych,
   b. prywatnych.

Rozdział 2. Zastosowanie

Do niniejszych wytycznych zobowiązani są stosować się wszyscy upoważnieni przez Dyrektora Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy do przetwarzania danych osobowych (pracownicy etatowi, zleceniobiorcy, stażyści, itd.), jeśli to przetwarzanie ma miejsce poza siedzibą Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy.

Rozdział 3. Definicje

- ✓ **Administrator** – Dyrektor Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy;
- ✓ **Bezpośredni przełożony** – osoba mająca prawo wydawania poleceń służbowych pracownikowi;
- ✓ **Dane osobowe** – dane osobowe, dla których Administratorem jest Dyrektor Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy;
- ✓ **Dokument** – informacja utrwalona w formie papierowej lub elektronicznej (na elektronicznym urządzeniu przenośnym);
- ✓ **Elektroniczne urządzenie przenośne** (elektroniczny nośnik danych) – urządzenie pozwalające przechowywać i odczytywać pliki, informacje i dokumenty w formie cyfrowej (elektronicznej), np. komputer przenośny – laptop, tablet, telefon, dysk zewnętrzny, pendrive;
- ✓ **IOD** – Inspektor Ochrony Danych – osoba wyznaczona przez Administratora, powołana do monitorowania i kontrolowania zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy;
- ✓ **Obszar przetwarzania danych osobowych** – pomieszczenia Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy, w których dochodzi do przetwarzania danych osobowych;
- ✓ **PBI**– zarządzenie nr 12/2021 Dyrektora Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy z dnia 31 marca 2021 r. w sprawie Polityki Bezpieczeństwa Informacji (PBI) Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy;
- ✓ **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- ✓ **Użytkownik** – osoba upoważniona przez Administratora do przetwarzania danych osobowych, użytkująca dokumenty i nośniki zawierające dane osobowe, dla których Administratorem jest

Dyrektor Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy;

✓ **Biblioteka** – Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy.

Rozdział 4. Założenia i wymogi formalne

W trakcie realizowania zadań związanych z funkcjonowaniem Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy (służbowych, wynikających z realizacji umów cywilnoprawnych, itp.) czasem występuje konieczność wyniesienia dokumentów i urządzeń zawierających dane osobowe poza obszary przetwarzania danych, w celu np. przeniesienia ich do innej lokalizacji, wykonywania pracy w domu, itp.
Ww. dokumenty i urządzenia zawierające dane osobowe mogą być wynoszone poza Bibliotekę zgodnie z zasadami określonymi w niniejszym dokumencie, tj. z zachowaniem należytej staranności i uwagi, oraz – w przypadku etatowych pracowników, wyłącznie za wiedzą i zgodą lub na polecenie bezpośredniego przełożonego. Przetwarzanie danych osobowych na elektronicznych urządzeniach przenośnych powinno być ograniczone tylko do niezbędnych przypadków i musi wynikać bezpośrednio z konieczności realizacji zadań i obowiązków służących zapewnieniu ciągłości funkcjonowania Biblioteki.
Każdy użytkownik, który przetwarza dane osobowe poza obszarami przetwarzania danych osobowych, ponosi całkowitą odpowiedzialność za bezpieczeństwo powierzonych mu dokumentów, sprzętu i nośników oraz danych osobowych tam zawartych, a także jest zobowiązany do stosowania się do niniejszych zasad.

Nie wolno wynosić poza Bibliotekę dokumentów zawierających dane szczególnych kategorii (np. dane o zdrowiu, dane wrażliwe), chyba że Dyrektor wyrazi pisemną zgodę. Wynoszenie danych zwykłych (np. dane czytelników, dane kontaktowe) jest dopuszczalne wyłącznie w zakresie niezbędnym do realizacji obowiązków służbowych.

Rozdział 5. Zabezpieczenia i wymogi techniczne

Wszelkie wynoszone dokumenty i nośniki danych, a także sprzęt wykorzystywany poza obszarem przetwarzania danych osobowych, muszą zostać odpowiednio zabezpieczone w sposób zapewniający przetwarzanym na nich danym osobowym:

- dostępność (czyli zabezpieczenie przed kradzieżą, utratą czy zniszczeniem),
- integralność (czyli uniemożliwienie zmiany treści danych/zawartości dokumentów lub nośników przez osobę nieuprawnioną),
- poufność (czyli zabezpieczenie treści danych/zawartości dokumentów lub nośników przed dostępem osób nieuprawnionych).

W szczególności:

1. Dokumenty w formie papierowej powinny być umieszczane w koszulkach lub foliach, a następnie w twardych i zamykanych teczkach aktowych, zabezpieczających przed uszkodzeniami fizycznymi.
2. Zabezpieczenia (hasła, PIN-y) na służbowych elektronicznych urządzeniach przenośnych, w tym możliwość zastosowania mechanizmów kryptograficznych (szyfrujących), zapewniane są przez Dział Informatyki. Niedopuszczalne jest przetwarzanie danych osobowych na elektronicznych urządzeniach przenośnych, które pracują poza Biblioteką, w postaci niezaszyfrowanej. Użytkownik jest ponadto zobowiązany przestrzegać instrukcji producenta, dotyczących ochrony sprzętu, np. przed wystawieniem na działanie silnego pola elektromagnetycznego. W przypadku nieprawidłowego działania zabezpieczeń, użytkownik jest zobowiązany poinformować o tym Dział Informatyki i nie ma prawa dokonywać własnoręcznej naprawy czy modyfikacji konfiguracji i

zabezpieczeń na urządzeniu. Sprzęt elektroniczny wykorzystywany poza Biblioteką podlega ubezpieczeniu.

3. Zabezpieczenia na prywatnych elektronicznych urządzeniach przenośnych i stacjonarnych, zapewniane są przez właściciela sprzętu. Zaleca się korzystanie z maksymalnych dostępnych zabezpieczeń oraz szyfrowania przesyłanych plików tekstowych, zawierających dane osobowe.
4. Minimalne wymagania bezpieczeństwa dla prywatnych urządzeń wykorzystywanych do pracy: aktualny system operacyjny, aktualne oprogramowanie antywirusowe, hasło lub PIN do urządzenia, blokada ekranu oraz szyfrowanie dysku. Korzystanie z urządzeń niespełniających tych wymagań jest zabronione.

Rekomenduje się, aby wybierając właściwe zabezpieczenia uwzględnić możliwe ryzyka np. uszkodzeń, kradzieży lub podsłuchu, które mogą różnić się w zależności od miejsca wykorzystywania sprzętu.

Rozdział 6. Czynności związane z przetwarzaniem poza Biblioteką:

Rozdział 6.1. Transport (przenoszenie, przewożenie)

1. Dokumenty papierowe i elektroniczne urządzenia przenośne mogą być transportowane wyłącznie w zamkniętej torbie/plecaku/walizce/skrzyni, uniemożliwiających łatwe poznanie ich zawartości. Niedozwolone jest ich przenoszenie w zewnętrznych kieszeniach ubrań, reklamówkach, workach foliowych lub torbach nieposiadających zamknięcia, a także w inny sposób mogący skutkować ich uszkodzeniem/zniszczeniem/zalaniem (np. ze względu na warunki atmosferyczne). Torba/plecak/walizka/skrzynia musi przez cały czas znajdować się pod bezpośrednią kontrolą użytkownika i w zasięgu jego wzroku.
2. W przypadku transportowania dużej ilości dokumentów w formie papierowej i/lub kilku elektronicznych urządzeń przenośnych (tj. takiej ich ilości, która nie zmieści się w jednej torbie/plecaku/walizce/skrzyni), powinno odbywać się to w asyście innej osoby (osób) upoważnionej (upoważnionych), przy użyciu stosownej liczby toreb/plecaków/walizek/skrzyń, zapewniających odpowiednie zabezpieczenie dokumentów i elektronicznych urządzeń przenośnych.
3. Zaleca się przewożenie znacznej ilości dokumentów papierowych i/lub elektronicznych urządzeń przenośnych przy wykorzystaniu pomocy pracowników korzystających za zgodą pracodawcy z samochodów prywatnych do celów służbowych.
4. W przypadku korzystania ze środków komunikacji publicznej/taksówek, należy zachowywać szczególną ostrożność.
5. Niedopuszczalne jest przekazywanie torby/plecaka/walizki/skrzyni, zawierającej dokumenty i/lub elektroniczne urządzenia przenośne w bezpośrednie władanie osób postronnych ani informowanie tych osób o ich zawartości.
6. Niedopuszczalne jest pozostawianie torby/plecaka/walizki/skrzyni bez nadzoru, np. w szatni, depozycie, samochodzie (w widocznym miejscu).

Rozdział 6.2. Przechowywanie

1. Dokumenty i elektroniczne urządzenie przenośne, które zostały wyniesione poza obszar przetwarzania, muszą być przechowywane w miejscu odpowiednio zabezpieczonym przed dostępem osób nieupoważnionych lub osób trzecich, a także uszkodzeniami fizycznymi.
2. Niedopuszczalne jest pozostawianie dokumentów i elektronicznych urządzeń przenośnych bez nadzoru w prywatnych mieszkaniach osób trzecich, recepcjach, oddawanie w depozyt, itp.
3. Niedopuszczalne jest przechowywanie środków dostępu do dokumentów i/lub elektronicznych urządzeń przenośnych (np. kluczy do toreb, haseł dostępu do komputera, PIN-u do telefonu) bezpośrednio przy dokumentach i/lub sprzęcie.

Rozdział 6.3. Korzystanie

1. Dokumenty i urządzenia elektroniczne powinny być przygotowywane do pracy (wyjmowane z teczek, uruchamiane) wyłącznie na czas pracy i niezwłocznie chowane, wyłączane (wygaszane, szyfrowane) po zakończeniu pracy.
2. Po ustaniu konieczności przetwarzania danych osobowych, należy je niezwłocznie trwale zniszczyć lub usunąć z elektronicznego urządzenia przenośnego lub stacjonarnego w sposób trwały. Dokumenty papierowe po zakończeniu pracy należy zwrócić do Biblioteki i/lub zniszczyć wyłącznie w służbowej niszczarce lub poprzez usługę profesjonalnej utylizacji. Niszczenie w domu (np. ręczne, w domowej niszczarce) jest zabronione.
3. W przypadku korzystania z prywatnych elektronicznych urządzeń przenośnych i stacjonarnych, będących własnością użytkownika, przez osoby inne niż użytkownik, należy założyć osobne, zahasłowane profile na tych urządzeniach, ograniczające nieuprawnionym osobom – w tym członkom rodziny – dostęp do zasobów służbowych przechowywanych na tych urządzeniach. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich, identyfikator oraz hasło do profilu, o którym mowa w zdaniu poprzedzającym i ponosi za to odpowiedzialność.
4. Niedopuszczalne jest współdzielenie służbowego elektronicznego urządzenia przenośnego z osobami nieuprawnionymi, a także zapoznawania ich z treścią dokumentacji.
5. Niedopuszczalne jest korzystanie na służbowym elektronicznym urządzeniu przenośnym z niezabezpieczonych, publicznych sieci Wi-Fi. Nie zaleca się korzystania z takich sieci na prywatnym elektronicznym urządzeniu przenośnym.
6. Niedopuszczalne jest samodzielne instalowanie na służbowym elektronicznym urządzeniu przenośnym jakichkolwiek programów czy aplikacji ani łączenie ich z innymi nieznanymi i niezabezpieczonymi urządzeniami elektronicznymi.
7. Niedopuszczalne jest korzystanie z dokumentacji i elektronicznych urządzeń przenośnych w bezpośredniej obecności osób nieuprawnionych, w sposób naruszający zasady określone w Rozdziale 5, lub stwarzający ryzyko takiego naruszenia. Szczególną ostrożność należy zachować w środkach komunikacji publicznej.
8. Przesyłanie danych osobowych poza Bibliotekę jest dopuszczalne wyłącznie za pomocą służbowej poczty e-mail lub innych narzędzi zatwierdzonych przez Bibliotekę. Zabrania się używania prywatnych adresów e-mail, komunikatorów internetowych lub niezabezpieczonych platform do przesyłania danych osobowych.
9. Zabrania się przechowywania danych osobowych na prywatnych usługach chmurowych (np. prywatny OneDrive, Dropbox, Google Drive) lub w aplikacjach niezatwierdzonych przez Bibliotekę.
10. W miejscach pracy poza Biblioteką należy stosować zasadę „czystego biurka i czystego ekranu", tj. nie pozostawiać dokumentów bez nadzoru, a ekran urządzenia blokować za każdym razem, gdy użytkownik odchodzi od stanowiska.

Rozdział 7. Wskazówki i uwagi

W przypadku utraty/zniszczenia/zagubienia dokumentów i/lub elektronicznych urządzeń przenośnych lub wystąpienia innych okoliczności stwarzających ryzyko naruszenia ochrony danych osobowych w związku z przetwarzaniem danych osobowych poza obszarami przetwarzania, należy postępować zgodnie z zasadami określonymi w pkt. 9 PBI oraz załącznikiem nr 11 do PBI, udostępnionymi na stronie http://pracownicy.bppragapd.pl/

Rozdział 8. Wykaz zmian

Nr zmiany	Opis zmiany (było - jest)	Miejsce zmiany (strona, rozdział, ustęp)
1		
2		

Rozdział 9. Terminy przeglądów

Planowe przeglądy niniejszego dokumentu odbywają się w terminie jednego roku od daty zatwierdzenia.

Lp.	Data przeglądu	Wykonał (data, podpis)	Uwagi