

Załącznik Nr 1 do Zarządzenia Nr 12/2021
Dyrektora Biblioteki Publicznej
im. Zygmunta Jana Rumla w Dzielnicy
Praga-Południe m.st. Warszawy z dnia
31.03.2021 r.



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

**POLITYKA BEZPIECZEŃSTWA INFORMACJI (PBI)
BIBLIOTEKI PUBLICZNEJ IM. ZYGMUNTA JANA RUMLA
W DZIELNICY PRAGA-POŁUDNIE M.ST. WARSZAWY**

Warszawa, marzec 2021 r.

1. WSTĘP

1. Przez pojęcie „Polityka Bezpieczeństwa Informacji”, dalej zwana jako „PBI”, należy rozumieć zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz organizacji. Kierownictwo każdej jednostki organizacyjnej, zobowiązane jest przepisami prawa do stworzenia optymalnego modelu zabezpieczeń technicznych i elektronicznych przetwarzanych informacji. Klasyfikacja informacji w postaci aktywów relewantnych (istotnych z punktu widzenia organizacji) w płaszczyznach działania Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy (zwaną dalej BP), stanowi podstawowe zadanie osób zaangażowanych w procesie tworzenia zasad zabezpieczenia zasobów informacyjnych. Istotnym wyzwaniem jest kwalifikowanie kategorii potencjalnych zagrożeń integralności informacji, w coraz większym stopniu instytucje, ich systemy i sieci informatyczne stają w obliczu zagrożeń pochodzących z rozmaitych źródeł, takich jak oszustwa dokonywane za pomocą komputerów, komunikatorów, urządzeń mobilnych oraz sieci. Szpiegostwo, sabotaż, wandalizm, pożar lub powódź to zjawiska aktywnej lub losowej utraty informacji oraz danych istotnych w procesie dostarczania usług. Poufność, dostępność i integralność informacji przy zachowaniu jej autentyczności, rozliczalności oraz niezaprzeczalności ma podstawowe znaczenie dla utrzymania płynności finansowej, zgodności z przepisami prawa oraz wizerunku jednostki.
2. Dokument PBI zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń w BP. Jednocześnie deklaruje zaangażowanie kierownictwa BP i wyznacza systematyczne procesowe podejście instytucji do zarządzania bezpieczeństwem informacji.
3. Omawiane zasady opierają się na obowiązujących uregulowaniach prawnych w BP, a należą do nich w szczególności:
 - a) ochrona danych osobowych i prywatności osób,
 - b) ochrona dokumentów finansowych BP,
 - c) prawa własności intelektualnej,
 - d) dokumenty związane z PBI, w szczególności IZSI,
 - e) odpowiedzialność związana z bezpieczeństwem informacji,
 - f) edukacja użytkowników w dziedzinie bezpieczeństwa informacji,
 - g) wsparcie i zaangażowanie kadry kierowniczej,
 - h) systematyczne i planowane w zakresie potrzeb, upowszechnianie wytycznych dotyczących PBI wśród wszystkich osób zaangażowanych w procesach przetwarzania informacji,
 - i) zgłaszanie przypadków naruszenia bezpieczeństwa informacji,
 - j) ocena zjawisk i potencjalnych zagrożeń.
4. Głównym celem niniejszej PBI jest organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych (informacji) oraz planowane w wymiarze BP kształcenie użytkowników

systemu ochrony bezpieczeństwa informacji, w zróżnicowanych wariantach prowadzonych zajęć (wewnętrzne instruktaże, analizy przypadków, omówienia zdarzeń).

5. PBI jest jednocześnie materiałem określającym zadania w zakresie właściwej realizacji poufności i integralności informacji przez nadanie uprawnień legalizujących przetwarzanie danych użytkownikom systemu ochrony informacji.
6. Niniejsza PBI została opracowana na podstawie Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

2. SŁOWNIK PODSTAWOWYCH POJĘĆ

Przez użyte w treści PBI sformułowania należy rozumieć:

1. **Administrator Systemu Informatycznego, dalej jako „ASI”** – pracownik wyznaczony przez ADO, odpowiedzialny za bezpieczeństwo i funkcjonowanie systemów informatycznych oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie,
2. **akceptowanie ryzyka** – decyzja, aby zaakceptować ryzyko,
3. **aktywa** – wszystko co ma wartość dla organizacji (zasoby),
4. **analiza ryzyka** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka,
5. **autentyczność** – właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane,
6. **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność,
7. **BP** – Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy przy ul. Janusza Meissnera 5, 03-982 – Administrator Danych Osobowych (ADO) w rozumieniu uodo, reprezentowany przez Dyrektora,
8. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w szczególności za dane osobowe uważa się: nazwisko, imię, nazwisko rodowe, PESEL, NIP, data zatrudnienia, wykształcenie, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, seria i numer dowodu osobistego, książeczki wojskowej, stan cywilny, płeć, adres zamieszkania lub pobytu, informacje o stanie zdrowia, nałogach, przynależności związkowej. BP przetwarza dane osobowe w formie tradycyjnej

- „T” (papierowej) oraz w formie elektronicznej – „E” (informatycznej), w granicach przepisów prawa,
9. **dostępność** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu,
 10. **elektroniczne nośniki informacji – „ENI”** – zewnętrzne nośniki danych, w szczególności płyty CD, DVD, PenDrive, pamięci typu FLASH, które muszą zostać zgłoszone i zarejestrowane przez ASI.
 11. **identyfikator użytkownika** – jest to ciąg znaków literowych (login) jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
 12. **incydent związany z bezpieczeństwem informacji** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji,
 13. **Inspektor Ochrony Danych Osobowych, dalej jako „IODO”** – pracownik osoba wyznaczona przez ADO, odpowiedzialny za zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych, nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz prowadzenie rejestru czynności przetwarzania danych przetwarzanych przez ADO, o którym mowa w art. 30 RODO, zawierającego informacje, o których mowa w art. 30 ust. 1 lit a-g RODO,
 14. **integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów,
 15. **IZSI** – Instrukcja Zarządzania Systemem Informatycznym obowiązująca w BP, stanowiąca Załącznik Nr 1 do niniejszej PBI,
Lokalny Administrator Bezpieczeństwa Informacji, dalej jako „LABI” – osoba odpowiedzialna za zabezpieczenie danych w powierzonym obszarze danych osobowych – kierownicy filii BP,
 16. **niezaprzeczalność** – brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
 17. **ocena ryzyka** – proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka,
 18. **Plan Ciągłości Działania** – cykliczne szkolenia użytkowników z ochrony danych osobowych, cykliczna analiza ryzyka u ADO, oraz czynności wynikające z IZSI,
 19. **postępowanie z ryzykiem** – proces wyboru i wdrażania środków modyfikujących ryzyko,
 20. **poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom,

21. **procesor** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
22. **przetwarzanie danych** – jakiegokolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
23. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
24. **rozliczalność** – funkcja umożliwiająca przypisanie w sposób jednoznaczny działania użytkownika lub podmiotu tylko temu użytkownikowi lub podmiotowi,
25. **sieć lokalna (intranet)** – połączenie jednostek komputerowych pracujących w BP w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,
26. **sieć publiczna** – publiczna sieć telekomunikacyjna, niebędąca siecią wewnętrzną wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu ustawy z dnia 16.07.2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 ze zm.),
27. **sieć telekomunikacyjna** – systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną rozumieniu ustawy z dnia 16.07.2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 ze zm.),
28. **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
29. **szacowanie ryzyka** – całościowy proces analizy i oceny ryzyka,
30. **UODO** – Urząd Ochrony Danych Osobowych, reprezentowany przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO) – organ do spraw ochrony danych osobowych, powoływany i odwoływany przez Sejm za zgodą Senatu,
31. **UODO** - ustawa z dnia 10.05.2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000),
32. **usuwanie danych osobowych** – rozumie się przez to zniszczenie zbiorów danych, danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
33. **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika,
34. **Użytkownik** – osoba upoważniona przez IODO do przetwarzania danych osobowych zarówno w systemach tradycyjnych „T” jak i w systemie informatycznym – elektronicznym „E” (pracownik, osoba wykonująca pracę na podstawie umowy cywilno-prawnej, osoba odbywająca staż pracy, praktykant),

- 35. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
- 36. **zakres upoważnienia** – należy przez to rozumieć zbieranie, opracowywanie, przechowywanie, zmienianie, usuwanie i udostępnianie danych,
- 37. **zakres upoważnienia/uprawnienia** – należy przez to rozumieć zbieranie, opracowywanie, przechowywanie, zmienianie, usuwanie i udostępnianie danych osobowych / informacji,
- 38. **zarządzanie ryzykiem** – skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem ryzyka,
- 39. **zdarzenie związane z bezpieczeństwem informacji** – jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem,

3. CEL ORAZ ZAKRES POLITYKI BEZPIECZEŃSTWA INFORMACJI – PBI

Nadrzędnym celem PBI BP jest:

- 1. Zapewnienie właściwej ochrony zasobów w BP.
- 2. Właściwy dobór zabezpieczeń (środków bezpieczeństwa) oparty na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań nadzoru, zobowiązań kontraktowych oraz pozostałych wymagań dotyczących bezpieczeństwa informacji w BP.

Zakres obowiązywania PBI BP:

- 1. Niniejszy dokument dotyczy wszystkich komórek organizacyjnych BP oraz wszystkich pracowników w rozumieniu ustawy Kodeks Pracy, a także innych osób mających dostęp do informacji chronionych w BP (np. pracowników firm zewnętrznych realizujących prace na rzecz BP).
- 2. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej, video lub innej).
- 3. Z dokumentem PBI są zobowiązani zapoznać się wszyscy pracownicy BP mający dostęp do danych osobowych/informacji.
- 4. PBI to system zapewniający poufność, dostępność i integralność informacji z uwzględnieniem dodatkowo takich atrybutów, jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność, oraz ciągłość działania.
- 5. Celem wdrożonej PBI jest osiągnięcie właściwego poziomu organizacyjnego i technicznego, który:
 - a) maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę BP,

- b) zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych (niepublicznych) oraz jawnych (publicznych),
 - c) zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów informatycznych przetwarzających informacje,
 - d) zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa BP, jego interesów, posiadanych i powierzonych jemu informacji oraz będzie gwarantem właściwej ochrony informacji oraz ciągłości procesu ich przetwarzania.
6. Realizacja wdrożonej w BP PBI odbywa się poprzez:
- a) określenie zgodnej z przepisami prawa, struktury organizacyjnej zapewniającej optymalny podział i koordynację zadań i odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji,
 - b) wyznaczenie lokalnie odpowiedzialnych funkcyjnych, dla kluczowych aktywów przetwarzania informacji, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa,
 - c) ciągle podnoszenie świadomości i kwalifikacji pracowników w obszarze bezpieczeństwa informacji.

4. ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI

1. Zarządzanie ryzykiem w BP opiera się na następujących zasadach:
- a) głównym elementem zarządzania aktywami i bezpieczeństwem informacji w BP jest przeprowadzanie okresowego szacowania ryzyka,
 - b) analiza jego wyników stanowi podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia ochrony zasobów BP,
 - c) szacowanie ryzyka bazuje na wytycznych normy PN-ISO/IEC 27005 lub przyjętej przez BP metodyce szacowania ryzyka dla bezpieczeństwa informacji. Podstawowym kryterium oceny ryzyka w BP jest eliminacja ryzyk o maksymalnej wartości z obszarów o największym ryzyku oraz eliminowanie ryzyka związanego z niezgodnością z regulacjami prawnymi,
 - d) szacowanie ryzyka jest przeprowadzane regularnie, nie rzadziej niż raz do roku, ryzyka są regularnie raportowane Kierownictwu BP,
 - e) cele stosowania zabezpieczeń i zabezpieczenia dobierane są przez BP adekwatnie do wymagań prawnych i wyników szacowania ryzyka dla bezpieczeństwa informacji,
2. Monitorowanie i przegląd bezpieczeństwa informacji w BP opiera się na zasadach:
- a) wykonywania audytów wewnętrznych, nie rzadziej niż raz na 12 miesięcy,
 - b) wykonywania bieżących przeglądów, dokonywanych przez kierownictwo BP.
3. Utrzymanie i doskonalenie bezpieczeństwa informacji w BP opiera się na następujących zasadach:
- a) przeprowadzania działań korygujących oraz oceny ich skuteczności,
 - b) przeprowadzania działań zapobiegawczych oraz oceny ich skuteczności,
 - c) informowania zainteresowanych stron o działaniach i udoskonaleniach.

4. Zarządzanie incydem w BP, związanym z bezpieczeństwem informacji prowadzone jest w ramach procesu zarządzania incydem i zostało opisane w rozdziale 8.
5. Nadzór nad dokumentacją w BP opiera się na następujących zasadach:
 - a) prowadzenia i nadzorowania dokumentacji systemowej,
 - b) prowadzenia i nadzorowania zapisów systemowych.
6. Zarządzanie dostępem do zasobów BP opiera się na następujących zasadach:
 - a) odbywa się w ramach procesu opartego na systemie obiegu wniosków o nadanie uprawnień do przetwarzania określonego rodzaju informacji,
 - b) procedury nadawania uprawnień do zasobów w ramach poszczególnych systemów informatycznych należy przeprowadzać zgodnie z IZSI.
7. Dokumentacja polityk bezpieczeństwa w BP funkcjonuje na następujących poziomach:
 - a) poziom BP – na poziomie BP ustanowiona została niniejsza PBI jako dokument systemowy o charakterze nadrzędnym względem pozostałych dokumentów w BP,
 - b) poziom systemów informatycznych – opisuje, w jaki sposób zasady i wymagania bezpieczeństwa zawarte w PBI i IZSI są realizowane w określonym systemie informatycznym,
 - c) poziom procedur, instrukcji i regulaminów wewnętrznych – procedury, instrukcje, regulaminy i inne dokumenty bezpieczeństwa informacji tworzone są w celu uszczegółowienia zasad opisanych w politykach.
8. Kierownicy komórek organizacyjnych BP odpowiadają za:
 - a) przeszkolenie instruktazowe pracowników w zakresie związanym z bezpieczeństwem informacji na stanowiskach pracy,
 - b) przestrzeganie zasad bezpieczeństwa informacji przez nich samych jak i przez podległych im pracowników,
 - c) identyfikowanie i dokumentowanie zagrożeń istotnych dla bezpieczeństwa informacji.
9. Zobowiązuje się kierowników komórek organizacyjnych, sporządzających projekty umów do zawierania w nich wymagań ochrony danych osobowych oraz bezpieczeństwa informacji w stopniu właściwym do zakresu umowy, a następnie ich przedkładania celem ostatecznej weryfikacji (akceptacji) oraz zaparafowania do IODO.
10. Odpowiedzialność za bezpieczeństwo informacji w BP ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków oraz uregulowaniami wewnętrznymi w przedmiotowej sprawie.
11. Każdy pracownik BP jest obowiązany dbać o bezpieczeństwo powierzonych mu do przetwarzania danych osobowych/informacji, zgodnie z obowiązującymi w BP przepisami wewnętrznymi, w tym w szczególności:
 - a) stosować zasady opisane w niniejszej PBI oraz innych dokumentach wewnętrznych BP, mających znaczenie z punktu widzenia bezpieczeństwa informacji,
 - b) chronić informacje istotne z punktu widzenia bezpieczeństwa informacji w BP przed dostępem do nich osób nieuprawnionych, przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,

- c) stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z PBI i IZSI BP,
- d) utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w BP,
- e) powiadomić IODO, ASI oraz bezpośredniego przełożonego o:
 - ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym,
 - nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian,
 - zniszczeniu lub możliwości zniszczenia informacji chronionych.

12. Podstawowe obowiązki w obszarze zarządzania bezpieczeństwem informacji w BP:

a) Administrator Danych Osobowych (ADO – BP):

- zatwierdza warunki techniczne i organizacyjne służące bezpieczeństwu informacji, w tym ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- decyduje o zakresie, celach oraz metodach przetwarzania i ochrony informacji, w tym danych osobowych,
- odpowiada za zgodne z prawem przetwarzanie informacji, w tym zasad obrotu i zabezpieczenia danych osobowych,
- Udziela IODO pełnomocnictwa do nadawania upoważnień do przetwarzania danych osobowych.
- Powołuje i odwołuje IODO.

b) Inspektor Ochrony Danych Osobowych – IODO:

- zapewnianie BP o przestrzeganiu przepisów o ochronie danych osobowych, w szczególności przez, sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- opracowanie w tym zakresie sprawozdania dla BP, nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- prowadzenie rejestru czynności przetwarzania danych przetwarzanych przez BP, zawierającego informacje, o których mowa w art. 30 ust. 1 lit a-g RODO,
- prowadzenie rejestru kategorii przetwarzania danych osobowych,
- nadawanie pracownikom w imieniu ADO uprawnienia do przetwarzania danych osobowych oraz prowadzenie ewidencji upoważnień,
- prowadzenie ewidencji naruszeń bezpieczeństwa informacji.

c) Administrator Systemu Informatycznego – ASI:

- odpowiada za bezpieczeństwo, rozliczalność, niezaprzeczalność oraz integralność danych zgromadzonych w zbiorach danych za pomocą systemów informatycznych,

- zarządza bezpieczeństwem informacji, w tym ochroną danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami IODO,
- przygotowuje projekty, opisy przedmiotu zamówienia w przypadku planowanych zakupów urządzeń wsparcia wydajności systemu informatycznego BP,
- przydziela identyfikatory (loginy) użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
- prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierające informacje chronione, w tym dane osobowe,
- nadaje lub odbiera uprawnienia oraz prowadzi ewidencję nadanych uprawnień do dostępu do aktywów,
- prowadzi nadzór nad przygotowaniem oraz aktualizacją IZSI,
- prowadzi nadzór nad przygotowaniem dokumentów planów ciągłości działania dla systemów informatycznych,
- zatwierdza i wprowadza plany awaryjne dla systemów informatycznych, nad którymi sprawuje nadzór,
- zarządza kopiami awaryjnymi danych, w tym danych osobowych zgodnie z otrzymanym upoważnieniem,

d) Użytkownik:

- odpowiada za poprawność merytoryczną danych gromadzonych w zbiorach danych za pomocą systemów informatycznych,
- chroni prawo do prywatności osób fizycznych powierzających BP swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w niniejszej PBI, IZSI,
- stosuje zabezpieczenia dla zasobów, do których ma dostęp,
- podejmuje odpowiednie działania w przypadku wykrycia naruszeń bezpieczeństwa informacji, zgodnie z IZSI,
- współpracuje z osobami pełniącymi rolę odpowiedzialne za bezpieczeństwo informacji tj. z IODO i ASI w zakresie realizacji zadań dotyczących bezpieczeństwa informacji.

5. BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

1. Pracownicy i procesorzy mający dostęp do informacji poufnych, podpisują porozumienia o zachowaniu poufności i nieujawnianiu informacji przed uzyskaniem dostępu do środków przetwarzania informacji.
2. Każda osoba upoważniona przez IODO do przetwarzania danych osobowych otrzymuje upoważnienie, zawierające datę wydania i wygaśnięcia upoważnienia, identyfikator, (jeśli dane osobowe przetwarzane są w systemie informatycznym), zakres przetwarzania danych osobowych. Wzór upoważnienia stanowi Załącznik Nr 2 do niniejszej PBI.
3. Dodatkowo upoważnienie zawiera oświadczenie o odpowiedzialności pracownika w razie ew. naruszeń, podpisywane przez pracownika.
4. IODO - organizuje szkolenia dla pracowników, którzy przetwarzają dane osobowe.

5. Kierownicy wprowadzają swoich pracowników i procesorów w swoje obowiązki i odpowiedzialność związaną z bezpieczeństwem danych osobowych przed nadaniem upoważnienia oraz przyznaniem im dostępu do poufnych informacji lub systemów informatycznych
6. W celu budowania świadomości pracowników, osoby upoważnione do przetwarzania danych osobowych przechodzą szkolenie wstępne a także dalsze szkolenia, prowadzone m.in. przez IODO. IODO pełni także funkcję doradczą dla pracowników BP.
7. Szkolenia obejmują odpowiedzialność pracowników, zapoznanie ich z obowiązującymi przepisami prawa, bezpieczne poruszanie się w sieci informatycznej, pogłębianie świadomości konieczności ochrony danych, wzmacnianie właściwych nawyków, zapoznanie z obowiązującymi w BP procedurami w przypadku naruszenia bezpieczeństwa informacji oraz wdrożenia Planu Ciągłości Działania. Każdy uczestnik szkolenia otrzyma zaświadczenie o odbyciu szkolenia z zakresu ochrony danych osobowych w bibliotece, zgodnie z wzorem, stanowiącym Załącznik Nr 3 do niniejszej PBI.
8. Po ustaniu zatrudnienia pracownicy w dalszym ciągu przestrzegają zasady o zachowaniu poufności, w szczególności wobec środków zabezpieczających dane w wersji tradycyjnej i elektronicznej.
9. Nadanie nowego upoważnienia do przetwarzania danych osobowych, np. w przypadku zmiany stanowiska lub zakresu obowiązków, powoduje wygaśnięcie obowiązywania dotychczasowego upoważnienia.
10. Dział Kadr jest zobowiązany niezwłocznie poinformować IODO oraz ASI o rozwiązaniu umowy o pracę z pracownikiem BP oraz o wszystkich nieobecnościach trwających powyżej 30 dni kalendarzowych.
11. Kandydat przed przystąpieniem do pracy jest zobowiązany przejść stosowne procedury podczas rozpoczęcia zatrudnienia (np. sprawdzić stan zdrowia u lekarza medycyny pracy, przejść szkolenie BHP, szkolenie z zakresu bezpieczeństwa informacji) oraz zapoznać się z obowiązującymi regulacjami wewnętrznymi, a w szczególności z niniejszą PBI, IZSI. Fakt zapoznania się dokumentami, o których mowa w zdaniu poprzedzającym powinien zostać potwierdzony własnoręcznym podpisem pracownika (na oświadczeniu bądź bezpośrednio na dokumencie np. zakresie obowiązków).

6. INWENTARYZACJA AKTYWÓW

A. ZARZĄDZANIE AKTYWAMI

BP zarządza swoimi aktywami (zasobami) w celu zapewnienia im wymaganego poziomu bezpieczeństwa informacji.

1. Do szczególnie chronionych aktywów w BP zalicza się:
 - a) **użytkowników** – kapitał wiedzy, jaki reprezentują,
 - b) **aktywa fizyczne** – zbiory biblioteczne, sprzęt informatyczny oraz nośniki danych,
 - c) **usługi** – usługi przetwarzania informacji, przesyłania informacji, usługi ogólne np. zasilanie,

- d) **oprogramowanie** – aplikacje, systemy operacyjne,
 - e) **informacje i procedury wewnętrzne** – bazy danych i pliki z danymi, polityki, regulaminy, instrukcje, umowy z dostawcami, dokumentacje systemów, plany ciągłości działania, plany odzyskiwania danych po awarii, logi systemowe i aplikacyjne oraz informacje przechowywane w kopiach zapasowych,
 - f) **wartości niematerialne** – dobre imię BP na zewnątrz, reputacja BP.
2. Każde nowe lub zmienione urządzenie (aktywo) służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji musi zostać zweryfikowane na zgodność z wymaganiami IZSI i dopuszczone do stosowania w BP, po wcześniejszym zaakceptowaniu przez ASI.
 3. Aktywa w BP są chronione na mocy: przepisów prawa (np. dane osobowe, informacje niejawne, prawo autorskie, dane finansowo-księgowe, zbiory biblioteczne), warunków licencji, zapisów umów pomiędzy BP a firmami zewnętrznymi.
 4. Wykaz budynków, w których przetwarzane są dane osobowe, są wyszczególnione w załączniku do IZSI.
 5. Wykaz zbiorów osobowych w postaci dokumentacji papierowej i elektronicznej zawierającej dane osobowe wraz ze wskazaniem programów służących do ich przetwarzania opisany jest w Załączniku Nr 4 do niniejszej Polityki.
 6. Rejestr czynności przetwarzania danych osobowych stanowi Załącznik Nr 5 do niniejszej Polityki.

B. ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

W BP przetwarza się następujące rodzaje informacji, ważnych z punktu widzenia bezpieczeństwa informacji:

- a) **dane osobowe** - za organizację systemu ochrony danych osobowych odpowiada BP – Administrator Danych Osobowych, który wykonuje swoje zadania wynikające z ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. 2018, poz. 1000). i rozporządzenia RODO przy pomocy IODO oraz ASI,
- b) **inne dane, stanowiące tajemnice ustawowo chronione:**
 - **tajemnica skarbową**, którą objęte są indywidualne dane zawarte w deklaracji oraz innych dokumentach składanych przez BP na podstawie art. 34 ustawy z dnia 28.09.1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41 poz. 214 ze zm.) oraz art. 293 – 305 ustawy z dnia 29.08.1997 r. Ordynacja podatkowa (Dz. U. z 2012 r. poz. 749 ze zm.),
 - **tajemnica przedsiębiorstwa**, którą objęte są nieujawnione do wiadomości publicznej informacje techniczne, organizacyjne BP lub inne informacje posiadające wartość handlową, dla których BP podjął niezbędne działania w celu zachowania ich poufności na podstawie art. 11 ust. 4 ustawy z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153 poz.1503 ze zm.),
 - **tajemnica pracodawcy** – BP, którą są tajemnice określone w odrębnych przepisach, na podstawie art. 100 ustawy z dnia 26.06.1974 r. Kodeks pracy (Dz. U. z 2014 r. poz. 1502 ze zm.).

- c) **informacja publiczna** to każda informacja o sprawach publicznych BP, która podlega udostępnieniu i ponownemu wykorzystywaniu na zasadach i w trybie określonych w ustawie z dnia 06.09.2001 r. o dostępie do informacji publicznej (Dz. U. z 2014 r. poz. 782 ze zm.).
2. Wszelkie informacje tworzone, przekazywane i przetwarzane w BP, nieoznaczone jako należące do osób trzecich, stanowią własność BP i podlegają ochronie.
 3. Informacje do użytku wewnętrznego można przetwarzać i przekazywać na zewnątrz BP tylko w ramach wykonywania obowiązków służbowych (informacja chroniona może być przekazywana jedynie do instytucji, osób, firm i organizacji współpracujących z BP lub uprawnionych przepisami prawa).
 4. Informacje do użytku wewnętrznego nie powinny być udostępniane poza BP.
 5. Informacja publiczna w BP, która nie została udostępniona w Biuletynie Informacji Publicznej jest udostępniana na wniosek strony.
 6. Klasyfikacja informacji - informacje publiczne (niechronione):
 - a) każda informacja o sprawach publicznych, zamieszczana w BIP BP,
 - b) wszystkie informacje tworzone, przekazywane i przetwarzane w BP, nieoznaczone, jako należące do osób trzecich i niesklasyfikowane, jako chronione,
 - c) publikacje na stronie internetowej BP.
 7. Klasyfikacja informacji - informacje do użytku wewnętrznego BP (chronione):
 - a) wewnętrzna komunikacja, korespondencja, poczta elektroniczna,
 - b) dane wewnętrzne takie jak: oferty, raporty, ceny,
 - c) dane osobowe czytelników oraz pracowników BP,
 - d) wewnętrzne dokumenty takie jak: wytyczne, instrukcje, plany organizacyjne,
 - e) fragmenty umów zawierające tajemnicę przedsiębiorstwa oferenta,
 - f) informacje powierzone przez strony trzecie,
 - g) dokumentacja projektowa,
 - h) publikacje w intranecie BP,
 - i) dane o środkach bezpieczeństwa, podatnościach, konfiguracji sieci,
 - j) kopie zapasowe i archiwalne zawierające informacje chronione,
 - k) dane dotyczące innych firm, w tym umowy o zachowaniu informacji w poufności,
 - l) wszelkie informacje związane z dokonywanymi operacjami bankowymi,
 - m) dane stojące na straży konkurencyjności postępowania przetargowego, dane przetargowe przed ich ostateczną publikacją na stronie internetowej BP,
 - n) hasła, kody dostępu, klucze szyfrujące stosowane w systemach informatycznych BP.
 8. Pełna inwentaryzacja aktywów wspierających znajduje się w IZSI.
 9. Publikowanie wizerunku osoby odbywać się może jedynie za jej zgodą, wzór zgody Czytelnika na publikowanie wizerunku stanowi Załącznik Nr 6.

7. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. W zakresie środków organizacyjnych BP, w drodze zarządzenia wdraża:
 - a) niniejszą PBI,
 - b) IZSI,
 - c) upoważnienia do przetwarzania danych osobowych/informacji,
 - d) ewidencję osób upoważnionych do przetwarzania danych osobowych/informacji,
 - e) umowy powierzenia przetwarzania danych osobowych z procesorami.
2. W zakresie środków technicznych BP, za pośrednictwem IODO oraz ASI wdraża:
 - a) kontrolę dostępu do obszarów przetwarzania danych osobowych,
 - b) zabezpieczenia przed utratą danych (np. zapasowe zasilanie, wykonywanie kopii zapasowych itp.),
 - c) urządzenia, dyski lub inne elektroniczne nośniki informacji (ENI), zawierające dane osobowe/informacje, przeznaczone do likwidacji, przekazania podmiotowi nieuprawnionemu do przetwarzania danych osobowych, naprawy — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
3. BP dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i zapewnia, aby dane te były:
 - a) przetwarzane zgodnie z prawem,
 - b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
 - c) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
 - d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
4. Pracownicy/osoby przetwarzające dane osobowe/informacje w systemach informatycznych w BP są zobowiązane do postępowania zgodnie z IZSI.
5. Pracownicy/osoby przetwarzające dane osobowe/informacje w BP są zobowiązane powiadomić IODO lub ASI o ewentualnych incydentach/zdarzeniach dotyczących bezpieczeństwa systemu ochrony danych osobowych/informacji we wszystkich zbiorach.
6. Zabrania się w BP przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, chyba że ich przetwarzanie jest dopuszczalne w świetle przepisów prawa powszechnie obowiązującego.
7. Zabrania się przetrzymywania dowodów osobistych czytelników w czytelniach pod zastaw.
8. Zabrania się korzystania z prywatnych telefonów komórkowych, komputerów oraz elektronicznych nośników informacji do celów służbowych, w szczególności do robienia zdjęć

pomieszczeniom, dokumentacji, uczestnikom spotkań/wydarzeń organizowanych przez BP. ADO może wyrazić zgodę na korzystanie z prywatnych telefonów komórkowych, komputerów oraz elektronicznych nośników informacji do celów służbowych w szczególnych przypadkach (praca zdalna, współpracownicy).

9. Dane osobowe przetwarzane przez BP mogą być uzyskiwane:
 - a) bezpośrednio od osób, których te dane dotyczą,
 - b) z innych źródeł, nie od osoby, której dotyczą w granicach dozwolonych przepisami prawa.
10. Zbierane dane osobowe mogą być wykorzystane tylko do celów, w jakich są lub będą przetwarzane. Po zakończeniu przetwarzania danych osobowych, powinny one być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą lub usunięte.
11. Pracownicy BP przetwarzający dane osobowe są odpowiedzialni w momencie zbierania danych od osoby, której one dotyczą za poinformowanie tej osoby o: tożsamość i dane kontaktowe ADO oraz tożsamość i dane kontaktowe Dyrektora BP, dane kontaktowe Inspektora Ochrony Danych, cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania, informacje o odbiorcach danych osobowych lub o kategoriach, wzmiankę o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych, okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu, informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, informacje o prawie wniesienia skargi do organu nadzorczego; informację, że podanie danych osobowych jest niezbędne do korzystania z zasobów, informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, zgodnie z wzorem stanowiącym Załącznik Nr 7 (Klauzula Informacyjna) do PBI,
12. Pracownicy BP uzupełniają kartę zobowiązań nowego Czytelnika według wzoru karty zobowiązań z Załącznika Nr 8 i.
13. Czytelnik, który chce usunąć swoje konto biblioteczne, przedkłada pracownikowi BP odpowiedniej jednostki (placówki, w której utworzono konto) wniosek o usunięcie konta, zgodnie ze wzorem z Załącznika Nr 9 do PBI.
14. Kandydaci składający dokumenty (podanie o przyjęcie do pracy w BP, list motywacyjny, CV) zobowiązani są do wyrażenia zgody na przetwarzanie ich danych osobowych w celach rekrutacyjnych. Osobom, których dane są przetwarzane w zbiorach BP przysługuje prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.
15. Każda osoba, która wystąpi z prośbą o otrzymanie informacji na temat jej danych lub z prośbą o skorzystanie z przysługujących jej praw, musi uzyskać odpowiedź na piśmie w terminie nieprzekraczającym 30 dni od daty wpływu prośby.

16. W przypadku, gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem RODO albo są zbędne do realizacji celu, dla którego zostały zebrane, bezpośredni użytkownik jest zobowiązany do ich uzupełnienia, uaktualnienia, spróśowania, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia. Przedmiotowych czynności dokonuje bezpośredni użytkownik pod nadzorem IODO.
17. Kierownik komórki organizacyjnej jest zobowiązany do wystąpienia do IODO z wnioskiem o wydanie stosownego upoważnienia, dla pracownika działu, który będzie przetwarzał dane osobowe, Pracownicy zatrudnieni na samodzielnych stanowiskach pracy występują we własnym imieniu z wnioskiem o wydanie stosownego upoważnienia, o którym mowa w zdaniu poprzedzającym.
18. IODO niezwłocznie rozpatruje wniosek, o którym mowa pkt. 16 i udziela upoważnienia do przetwarzania danych osobowych, zgodnie z wzorem stanowiącym Załącznik Nr 2 do PBI lub odmawia udzielenia upoważnienia podając w formie pisemnej motywy swojego rozstrzygnięcia Dyrektorowi BP.
19. Integralną częścią upoważnienia, o którym mowa w pkt. 16 jest podpisane przez każdą osobę przetwarzającą dane osobowe „Oświadczenie o zachowaniu w tajemnicy danych osobowych/informacji oraz sposobów ich zabezpieczenia”, którego wzór stanowi Załącznik Nr 2 do PBI.
20. W przypadku konieczności cofnięcia upoważnienia (zmiana stanowiska pracy, rozwiązanie stosunku pracy) do przetwarzania danych osobowych/informacji IODO dokonuje cofnięcia upoważnienia, zgodnie z wzorem stanowiącym Załącznik Nr 2 do PBI oraz występuje do ASI, w sytuacji przetwarzania przez pracownika danych osobowych w systemie informacyjnym o dokonanie odpowiedniej zmiany w ww. systemie – odebranie praw dostępu.
21. IODO prowadzi „Ewidencję osób upoważnionych do przetwarzania danych osobowych”, której wzór stanowi Załącznik Nr 10 do niniejszej PBI.
22. BP może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy powierzenia przetwarzania danych osobowych, przy zachowaniu postanowień art. 28 RODO.
23. Budynek, w którym znajdują się dane przetwarzane w systemie T i/lub E oraz pomieszczenia spełniają wymagania przeciwpożarowe zgodnie z instrukcją bezpieczeństwa pożarowego przewidzianą w BP.
24. Powyższe pomieszczenia, jako obszary przetwarzania danych osobowych w BP powinny być zamykane na czas nieobecności w nich pracowników/osób upoważnionych do przetwarzania danych osobowych w sposób uniemożliwiający dostęp do nich osób trzecich.
25. Dane osobowe przechowywane w systemie T są przechowywane po zakończeniu pracy w BP w danym pomieszczeniu w zamykanych na klucz meblach biurowych. Wszystkie klucze od szafek z danego pomieszczenia należy po zakończeniu pracy przechowywać w jednym miejscu (wybranej szafce lub szufladzie biurka, szafy). Przedmiotowe kwestie zostały szczegółowo uregulowane w obowiązującym Zarządzeniu Dyrektora BP w sprawie „Instrukcji postępowania z kluczami i kodami cyfrowymi do systemu alarmowego oraz zabezpieczenia pomieszczeń Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Pra-

- ga-Południe m. st. Warszawy”, W celu ochrony danych osobowych stosuje się następujące zabezpieczenia fizyczne:
- a) Serwery są zlokalizowane w pomieszczeniach biurowych, w których mogą znajdować się wyłącznie osoby upoważnione przez ADO,
 - b) Urządzenia systemu informatycznego BP są zasilane za pośrednictwem systemu podtrzymywania UPS oraz dedykowanego obwodu elektrycznego.
26. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej obejmują:
- a) BP wykorzystuje zaporę sieciową w celu separacji sieci lokalnej od sieci publicznej,
 - b) korzystanie z zasobów sieci wewnętrznej jest możliwe tylko po podaniu nazwy użytkownika i hasła,
 - c) ADO stosuje zabezpieczenie oprogramowaniem antywirusowym, by zminimalizować ryzyko ingerencji przez zewnętrzne ataki w systemy informatyczne;
27. Zestawienie środków technicznych i organizacyjnych w BP, niezbędnych dla zapewnienia poufności, integralności, dostępności danych osobowych/informacji przy uwzględnieniu ich autentyczności, rozliczalności oraz niezaprzeczalności w zakresie systemów elektronicznych zostało szczegółowo uregulowane w IZSI.
28. Każdy z systemów informatycznych przetwarzających dane osobowe w BP musi:
- a) umożliwiać dokonywanie wglądu, weryfikacji i poprawy przetwarzanych danych osobowych osobie, której te dane dotyczą,
 - b) umożliwiać trwałe usuwanie danych, dla których cel przetwarzania został osiągnięty,
 - c) umożliwiać wskazanie użytkownika odpowiedzialnego za wprowadzenie lub edycję danych wraz z podaniem daty i godziny operacji.
29. W BP należy regularnie monitorować wdrożone zabezpieczenia systemu informatycznego.

8. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

1. BP działaniami organizacyjnymi zapewnia wysoki poziom bezpieczeństwa fizycznego i środowiskowego.
2. Działaniami w zakresie zapewniania bezpieczeństwa fizycznego i środowiskowego w BP bezpośrednio kierują: Specjalista ds. Administracji BP w zakresie ochrony mienia oraz obiektu, natomiast w zakresie bezpieczeństwa środowiskowego, w szczególności ochrony przeciwpożarowej – pracownik zatrudniony na stanowisku ds. BHP i p.poż BP.
3. Specjalista ds. Administracji BP sprawuje nadzór funkcjonalny nad działaniami realizowanymi przez agencje ochrony zabezpieczające obiekty BP.
4. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w BP w odniesieniu do informacji.
5. Kluczowe systemy techniczne i informatyczne w BP wyposażone są w systemy utrzymujące optymalne warunki środowiskowe i podtrzymujące zasilanie.
6. Dokumenty zawierające informacje wrażliwe należy przechowywać w zamykanych na klucz szafach i meblach biurowych lub szafach metalowych na akta, do których dostęp mają wyłącznie pracownicy upoważnieni do przetwarzania danych osobowych. Pomiesz-

czenia, w których znajdują się szafy służące do przechowywania informacji wrażliwych, są wyposażone w system sygnalizacji pożaru.

7. Wadliwe wydruki i wersje robocze dokumentów zawierające dane osobowe zwykłe lub wrażliwe należy skutecznie niszczyć przy użyciu niszczarek. Uszkodzone dyski twarde, taśmy magnetyczne, płyty CD/DVD i inne komputerowe nośniki danych, zawierające informacje wrażliwe, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji.
8. Szczegółowo przedmiotowe zagadnienia zostały uregulowane w IZSI.

9. ZARZĄDZANIE INCYDENTAMI NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

1. Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego chronione informacje w BP jest każdy stwierdzony fakt nieuprawnionego ujawnienia informacji, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
 - a) nieautoryzowany dostęp do danych,
 - b) nieautoryzowane modyfikacje lub zniszczenie danych,
 - c) udostępnienie danych nieautoryzowanym podmiotom,
 - d) nielegalne ujawnienie danych,
 - e) pozyskiwanie danych z nielegalnych źródeł,
 - f) pozostawienie elektronicznych nośników informacji (ENI), w tym w szczególności przenośnych pamięci typu Flash na biurku pracownika po zakończeniu pracy albo w/na jednostce komputerowej,
 - g) pozostawienie kartki papieru zawierającej dane osobowe/informację na biurku pracownika po zakończeniu pracy albo w/na urządzeniu kserograficznym.
2. Każdy pracownik BP, który stwierdzi zdarzenie, względnie incydent związany z bezpieczeństwem informacji dokonany przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo informacji jest zobowiązany niezwłocznie zgłosić ten fakt IODO, a w razie jego nieobecności ASI.
3. W przypadku stwierdzenia naruszenia bezpieczeństwa informacji pracownik BP powinien zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IODO lub ASI.
4. W związku z sytuacją, o której mowa w ust. 3, IODO w porozumieniu z ASI podejmuje następujące czynności:
 - a) zapoznaje się z zaistniałą sytuacją (minimalizuje negatywne skutki zdarzenia, wyjaśnia okoliczności zdarzenia, zabezpiecza dowody zdarzenia oraz stara się umożliwić dalsze bezpieczne przetwarzanie danych) i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy BP,

- b) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
 - c) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu dyrekcję – kadrę zarządzającą BP,
 - d) nawiązuje kontakt ze specjalistami zewnętrznymi, jeśli zachodzi taka potrzeba,
 - e) może nakazać przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
5. Polecenia służbowe wydawane przez IODO w czasie realizacji zadań wynikających z niniejszej PBI muszą być wykonywane przed innymi zapewniając bezpieczeństwo danych osobowych.
 6. Obowiązkiem każdego użytkownika systemu jak i pracownika przetwarzającego dane osobowe w sposób tradycyjny jest realizacja zadań wynikających z niniejszej PBI oraz należyte zabezpieczenie interesów BP.
 7. Odmowa udzielenia wyjaśnień lub współpracy z IODO będzie traktowana jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
 8. IODO po zaistnieniu zdarzenia opracowuje „Raport z naruszenia bezpieczeństwa danych osobowych”, zgodnie z wzorem stanowiącym Załącznik Nr 11 do PBI, w którym przedstawia przyczyny i skutki zdarzenia, proponuje działania korygujące oraz zapobiegawcze, a także przedstawia wnioski końcowe, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości.
 9. IODO zasięga również niezbędnych opinii ekspertów zewnętrznych w zakresie odtworzenia działania systemu po nieoczekiwanej awarii i wznowienia przetwarzania danych osobowych/informacji zapewniając tym samym realizację zasady ciągłości działania BP, zgodnie z zapisami zarządzania ciągłością działania.
 10. IODO prowadzi „Rejestr naruszeń bezpieczeństwa informacji”, zgodnie z wzorem stanowiącym Załącznik Nr 12 do niniejszej PBI.

10. ZGODNOŚĆ Z PRZEPISAMI PRAWA I DOKUMENTAMI POWIĄZANYMI

1. BP dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów.
2. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawa karnego lub cywilnego, zobowiązań wynikających z ustaw, aktów wykonawczych, zarządzeń wewnętrznych BP lub umów ze stronami trzecimi oraz jakichkolwiek wymagań bezpieczeństwa informacji.
3. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności w BP związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji.

4. W BP prowadzony jest nadzór nad komplementarnością stosowanych rozwiązań technicznych urządzeń oraz przeprowadzane są okresowe weryfikacje wewnętrzne funkcjonowania systemu.
5. W BP informacje podlegają ochronie na podstawie następujących przepisów prawa, polskich norm oraz dokumentów powiązanych:
 - Ustawa z dnia 10.05.2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000 ze zm.)
 - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
 - Ustawa z dnia 06.06.1997 r. Kodeks karny (Dz. U. 2017 r. poz. 2204 ze zm.)
 - Ustawa z dnia 26.06.1974 r. Kodeks pracy (Dz. U. 2018 r. poz. 917 ze zm.)
 - Ustawa z dnia 23.04.1964 r. Kodeks cywilny (Dz. U. 2018 r. poz. 1025 ze zm.)

11. ZASADY ROZPOWSZECZNIA DOKUMENTU PBI ORAZ TRYB WPROWADZANIA ZMIAN

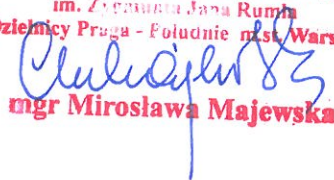
1. Z niniejszą PBI i dokumentami związanymi zobowiązani są zapoznać się: kadra zarządzająca, kadra kierownicza oraz pracownicy BP.
2. Niniejszy dokument może być udostępniony w celu zapoznania się i postępowania w zgodzie z zapisami niniejszej PBI, uprawnionym podmiotom zewnętrznym.
3. Zmiany w niniejszym dokumencie wprowadzane są zgodnie z procedurą zarządzania dokumentacją BP w formie stosownych aneksów do zarządzenia Dyrektora BP.
4. Nadzór nad przestrzeganiem niniejszej PBI oraz dokumentów z nią związanych pełni IO-DO.

12. POSTANOWIENIA KOŃCOWE

1. Nieprzestrzeganie postanowień zawartych w niniejszej PBI, a także brak nadzoru nad ochroną danych osobowych stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych w BP i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami ustawy z dnia 26.06.1974 r. Kodeks pracy (Dz. U. 2018 r. poz. 917 ze zm.).
2. Jeżeli skutkiem działania użytkownika jest ujawnienie informacji osobie nieupoważnionej, pracownik BP dopuszczający się takiego czynu może być pociągnięty do odpowiedzialności karnej określonej przepisami ustawy z dnia 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000 ze zm.) oraz ustawy z dnia 06.06.1997 r. Kodeks karny (Dz. U. 2017 r. poz. 2204 ze zm.).
3. Jeżeli skutkiem działania użytkownika jest powstanie szkody po stronie osoby, której dane osobowe się przetwarza(ło) lub osoby trzeciej, pracownik BP ponosi odpowiedzialność materialną na warunkach określonych w przepisach ustawy Kodeks pracy oraz stosowanymi odpowiednio zapisami ustawy z dnia 23.04.1964 r. Kodeks cywilny (Dz. U. 2018 r. poz. 1025 ze zm.).

Załączniki:

- 1) Instrukcja Zarządzania Systemem Informatycznym;
- 2) Wzór upoważnienia do przetwarzania danych osobowych;
- 3) Zaświadczenie o odbyciu szkolenia;
- 4) Wykaz zbiorów danych osobowych;
- 5) Wzór rejestru czynności przetwarzania;
- 6) Wzór zgody na publikację wizerunku;
- 7) Klauzula Informacyjna;
- 8) Karta zobowiązania;
- 9) Wzór wniosku o usunięcie konta bibliotecznego;
- 10) Ewidencja osób upoważnionych do przetwarzania danych osobowych;
- 11) Wzór Raportu o naruszeniu bezpieczeństwa danych osobowych;
- 12) Wzór Rejestru naruszeń bezpieczeństwa danych osobowych.

DYREKTOR BIBLIOTEKI PUBLICZNEJ
im. Zygmunta Jana Rumi
w Dzielnicy Praga - Południe m.st. Warszawy

mgr Mirosława Majewska

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 2021 r.

Spis treści

Cel i zakres stosowania instrukcji	3
Informacje ogólne	3
Definicje	3
Obowiązki z zakresu ochrony danych osobowych	5
Obowiązki Administratora Systemu	5
Obowiązki użytkowników	6
Nadawanie i odbieranie uprawnień do przetwarzania danych osobowych w systemach informatycznych	6
Nadawanie i rejestrowanie uprawnień	6
Wyrejestrowanie uprawnień	7
Metody i środki uwierzytelniania	8
Identyfikator	7
Hasło	7
Hasło administratora systemu	9
Procedura rozpoczęcia, zawieszenia oraz zakończenia pracy przez użytkowników systemu ...	8
Praca na stacjach roboczych	9
Praca na komputerach przenośnych	9
Procedura tworzenia kopii zapasowych	10
Częstotliwość wykonywania kopii	10
Przechowywanie kopii zapasowych	10
Testowanie kopii zapasowych	10
Likwidacja nośników zawierających kopie zapasowe	10
Procedura postępowania na wypadek wystąpienia awarii	10
Postępowanie w przypadku awarii jednostkowej	11
Postępowanie w przypadku awarii zwykłej	11
Postępowanie w przypadku awarii krytycznej	11
Zalecenia dalszego postępowania	11
Przechowywanie elektronicznych nośników informacji z danymi osobowymi	12
Sposób zabezpieczania systemu informatycznego przed działalnością oprogramowania, które może uzyskać nieuprawniony dostęp do danych osobowych	12
Kontrola nad wprowadzeniem, przetwarzaniem i udostępnianiem danych osobowych	12
Procedury wykonywania konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych	13
Naprawy urządzeń komputerowych z danymi osobowymi	14
Wymagania dotyczące sprzętu i oprogramowania	14
Harmonogram cyklicznego badania podatności systemów IT	15
Zakres badań	15
Przebieg badań	16
Postanowienia końcowe	16

CEL I ZAKRES STOSOWANIA INSTRUKCJI

Instrukcja określa sposób zarządzania systemem informatycznym, który służy do przetwarzania danych osobowych przez Administratora Danych. Celem niniejszej instrukcji jest wyeliminowanie zagrożeń związanych z udostępnieniem danych osobowych osobom nieupoważnionym, utratą lub uszkodzeniem danych.

Instrukcja przeznaczona jest dla wszystkich osób, które mają dostęp do danych osobowych w systemach informatycznych.

Informacje ogólne

1. Niniejsza Instrukcja Zarządzania Systemami Informatycznymi (IZSI) została opracowana na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 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. 2012 poz. 526 oraz Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
2. Wyznaczony Administrator Bezpieczeństwa Informacji będzie posiadał odpowiednie uprawnienia w nadzorowanych systemach informatycznych. Uprawnienia te zagwarantują skuteczne wykonywanie zadań z zakresu nadzoru nad przestrzeganiem przepisów prawa odnoszących się do ochrony danych osobowych. Uprawnienia w zakresie nadzoru nie oznaczają, że Administrator Bezpieczeństwa Informacji będzie miał automatyczny dostęp do przetwarzanych danych osobowych.
3. Za najważniejszy cel uznano zapewnienie bezpieczeństwa przetwarzanym danym osobowym.

Definicje

Ilekroć w niniejszej instrukcji będzie mowa o:

1. **IZSI** – Instrukcja Zarządzania Systemami Informatycznymi.
2. **Administrator Danych Osobowych (ADO)** – Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy, której przedstawicielem jest Dyrektor.
3. **Inspektor Ochrony Danych Osobowych (IODO)** – osoba, której Administrator Danych powierzył pełnienie obowiązków Inspektora Ochrony Danych Osobowych.
4. **Administrator Systemów Informatycznych (ASI)** – osoba odpowiedzialna za funkcjonowanie systemów informatycznych u Administratora Danych.

5. **Administrator Systemu Informatycznego SOWA SQL** – osoba odpowiedzialna za administrowanie systemem informatycznym SOWA SQL.
6. **Użytkownik (pracownik)** – osoba mająca dostęp do systemu informacyjnego na podstawie upoważnienia nadanego przez ADO lub IODO.
7. **Identyfikator** – jest to ciąg znaków literowo cyfrowych, który jednoznacznie identyfikuje użytkownika systemu informatycznego, który jest upoważniony do przetwarzania danych osobowych w systemie informatycznym.
8. **Hasło** – jest to ciąg znaków literowych, cyfrowych, specjalnych znany jedynie użytkownikowi.
9. **Integralność danych** – jest to właściwość, która zapewnia, że dane osobowe nie zostały zmienione, skasowane w nieautoryzowany sposób.
10. **Odbiorca danych** – jest to każdy, komu udostępniane są dane osobowe z wyjątkiem osoby, której te dane dotyczą, osoby upoważnionej do przetwarzania danych, podmioty, którym Administrator Danych powierzył przetwarzanie danych, organów państwowych, którym dane są udostępniane w związku z prowadzonym postępowaniem.
11. **Osoba upoważniona do przetwarzania danych** – jest to osoba, która uzyskała upoważnienie do przetwarzania danych przez Administratora Danych w formie pisemnej.
12. **Przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych.
13. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE .
14. **Serwisant** – osoba lub firma zajmująca się sprzedażą, instalacją, naprawą sprzętu komputerowego.
15. **Awaria** – należy przez to rozumieć stan niesprawności systemu informatycznego, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie.
16. **Awaria jednostkowa** – należy przez to rozumieć awarię o ograniczonym zakresie, dotyczącą zazwyczaj pojedynczego stanowiska lub użytkownika.
17. **Awaria zwykła** – należy przez to rozumieć awarię wpływającą na elementy systemu informatycznego, nie będącą awarią krytyczną, ani awarią jednostkową, zazwyczaj mającą wpływ na więcej niż jednego użytkownika, ale mniej niż 50% użytkowników systemu lub tylko część funkcji realizowanych przez system.
18. **Awaria krytyczna** – należy przez to rozumieć awarię systemu informatycznego lub przerwanie dostępu do Internetu w siedzibie głównej Biblioteki (serwerownia), uniemożliwiająca pracę co najmniej 50% użytkowników tego serwisu; awaria krytyczna uniemożliwia czasową lub trwałą eksploatację i wykonywanie wszystkich funkcjonalności przewidzianych dla systemu obsługi biblioteki.
19. **BP** – Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy.

OBOWIĄZKI Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

1. Do obowiązków osób przetwarzających dane osobowe w systemach informatycznych należy:
 - a) Przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych.
 - b) W przypadku naruszenia ochrony danych osobowych aktywne podjęcie współpracy z ADO, ABI oraz IODO, mające na celu usunięcie skutków naruszeń oraz zapobieganie ich wystąpieniu w przyszłości.
2. Użytkownicy (pracownicy) powinni przechodzić okresowe szkolenia związane z ewentualnymi zmianami w systemach informatycznych (zmiana wersji oprogramowania, wymiana sprzętu), zmiany wewnętrznych procedur, zmiany przepisów o ochronie danych osobowych.
3. W zakresie kompetencji osób zarządzających pracownikami jest wnioskowanie o nadawanie, zmianę, odebranie uprawnień do systemów informatycznych, w których przetwarzane są dane osobowe.
4. W sytuacji gdy obsługę informatyczną powierza się firmie zewnętrznej lub gdy systemy informatyczne należące do Administratora Danych znajdują się w firmach zewnętrznych, konieczne jest aby infrastruktura teleinformatyczna w tych firmach spełniała co najmniej standardy określone w tym dokumencie.

OBOWIĄZKI ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

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

1. Przestrzeganie opracowanych procedur operacyjnych oraz procedur bezpieczeństwa.
2. Zarządzanie systemami informatycznymi w taki sposób, aby zapewnić maksymalną ochronę danych osobowych.
3. Zarządzanie systemowymi środkami uwierzytelniania, a w szczególności zakładanie i blokowanie lub kasowanie użytkowników, a także dokonywanie zmian uprawnień na podstawie zaakceptowanych wniosków dostarczonych przez osobę upoważnioną.
4. Utrzymanie systemu w odpowiednim stanie technicznym.
5. Nadzorowanie przepływu informacji pomiędzy systemami informatycznymi a siecią publiczną.
6. Nadzorowanie bezpieczeństwa systemów informatycznych.
7. Tworzenie kopii zapasowych zasobów danych osobowych, programów służących do ich przetwarzania, a także okresowe weryfikowanie poprawności wykonywania kopii.
8. Nadzorowanie lub samodzielne wykonywanie okresowej konserwacji systemów informatycznych, w tym sprzętu, aplikacji, elektronicznych nośników informacji, na których przetwarzane są dane osobowe.

OBOWIĄZKI UŻYTKOWNIKÓW

Za użytkownika (pracownika) systemu uważa się każdą osobę mającą dostęp do systemu informatycznego, bez względu na formę zatrudnienia bądź współpracy z Biblioteką. Do obowiązków użytkownika systemu informatycznego, w których przetwarzane są dane osobowe należy:

1. Przestrzeganie zasad przetwarzania danych osobowych wdrożonych w instytucji.
2. Przestrzeganie opracowanych procedur operacyjnych oraz procedur bezpieczeństwa.
3. Zapobieganie dostępowi do danych osobowych przez osoby nieupoważnione.
4. Udostępnianie danych osobowych wyłącznie osobom upoważnionym do ich przetwarzania.
5. Niezwłoczne informowanie Inspektora Ochrony Danych Osobowych o każdym naruszeniu, podejrzeniu naruszenia i wszelkich innych nieprawidłowościach przy przetwarzaniu danych osobowych.
6. Niezwłoczne wykonywanie poleceń Inspektora Ochrony Danych Osobowych w zakresie ochrony danych osobowych, jeżeli są one zgodne z obowiązującymi przepisami prawa.

NADAWANIE I ODBIERANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

Nadawanie i rejestrowanie uprawnień

1. Każdy Użytkownik przed przystąpieniem do przetwarzania danych osobowych w systemach informatycznych zobowiązany jest zapoznać się z:
 - a) Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).
 - b) Polityką Bezpieczeństwa Informacji (PBI).
2. Każdy Użytkownik przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinien przejść szkolenie z zakresu obsługi sprzętu informatycznego, oprogramowania systemowego oraz aplikacji, których będzie używał.
3. Zarejestrowanie Użytkownika w systemie i nadanie mu stosownych uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożonym przez pracownika oświadczeniem o zachowaniu tajemnicy danych osobowych i sposobów ich zabezpieczania i pozyskaniem formalnego upoważnienia od Inspektora Ochrony Danych Osobowych do przetwarzania danych osobowych.
4. Identyfikator oraz zakres przyznanych uprawnień do przetwarzania danych dla Użytkownika powinien być zarejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych.
5. Procedurę nadania uprawnień do przetwarzania danych osobowych należy także stosować w przypadku zmiany lub odebrania uprawnień do systemów informatycznych.
6. Osobom, które nie są pracownikami etatowymi lub stałymi współpracownikami należy przyznawać czasowy dostęp do systemów informatycznych. Czas przyznania dostępu powinien pokrywać się z czasem wykonania zleconego zadania.

7. Dostęp do systemu informatycznego oraz do pojedynczych aplikacji i baz danych, w których przetwarza się dane osobowe powinien być możliwy po podaniu indywidualnego dla każdego użytkownika identyfikatora i hasła.
8. Dostęp do systemu informatycznego, który służy do przetwarzania danych osobowych powinien być możliwy tylko dla osób upoważnionych do przetwarzania danych osobowych, zarejestrowanych jako Użytkownik (pracownik) w tym systemie przez Administratora Danych Osobowych. Rejestracja powinna być możliwa tylko na pisemny wniosek bezpośredniego przełożonego, który także określa zakres uprawnień pracownika.
9. Rejestracja Użytkownika polega na utworzeniu identyfikatora i przydzieleniu jednorazowego hasła w systemie. Podczas pierwszego logowania, Użytkownik powinien zmienić hasło na nowe, takie, które tylko on będzie znał.
10. Każdy pracownik ponosi pełną odpowiedzialność za wszelkie operacje wykonane w systemie przy użyciu jego identyfikatora i hasła.
11. Pracownikowi wolno wykonywać tylko i wyłącznie te czynności, do których został upoważniony.
12. Każde przekroczenie lub próba przekroczenia nadanych uprawnień stanowić będą naruszenie obowiązków pracowniczych.
13. Każdy pracownik przetwarzający dane osobowe zobowiązany jest do zachowania tajemnicy zarówno w czasie zatrudnienia jak również po jego ustaniu.
14. W przypadku, gdy Administrator Systemów Informatycznych jest nieobecny dłużej niż 14 dni kalendarzowych, ADO zobowiązany jest do upoważnienia innej osoby na czas nieobecności ASI.
15. Osoby, które piastują kierownicze stanowiska w instytucji, zobowiązane są do informowania Inspektora Ochrony Danych Osobowych o każdej zmianie mającej wpływ na zakres uprawnień podległych pracowników.
16. Nadawanie, zmiana uprawnień (login i hasło) pracownikom obsługującym system informatyczny SOWA SQL mają osoby upoważnione przez ADO, tzw. administratorzy systemu informatycznego SOWA SQL.

Wyrejestrowanie uprawnień

1. Wyrejestrowania pracownika z systemu informatycznego dokonują osoby upoważnione przez ADO, po otrzymaniu wniosku od Kierownika Działu Kadr.

METODY I ŚRODKI UWIERZYTELNIANIA

Identyfikator

1. Identyfikator powinien składać się z ciągu znaków alfanumerycznych. Szczegółowe reguły tworzenia identyfikatora należą do obowiązków Administratora Systemów Informatycznych.



Hasło

1. Hasło powinno być unikatowym ciągiem minimum 8 znaków, zawierać duże i małe litery oraz cyfry. Używanie znaków specjalnych jest dodatkowo zalecane. Hasło nie może być identyczne lub podobne do identyfikatora użytkownika. Nie może być jego imieniem, nazwiskiem, datą urodzenia.
2. Stosowane hasła powinny być łatwe do zapamiętania, ale trudne do odgadnięcia. Nie powinny być powiązane z łatwymi do skojarzenia informacjami na temat użytkownika takimi jak numery telefonów, daty urodzenia dzieci, imiona dzieci itp.
3. System informatyczny powinien wymuszać zmianę hasła co 30 dni, w uzasadnionych przypadkach Administrator Systemów Informatycznych ma prawo do wymuszenia zmiany hasła w krótszym okresie.
4. W przypadku, gdy system informatyczny nie posiada funkcjonalności do wymuszania zmiany hasła, każdy użytkownik jest zobowiązany do samodzielnej zmiany hasła nie rzadziej niż co 30 dni.
5. Nie należy używać ponownie tych samych haseł.
6. Użytkownik ma bezwzględny zakaz udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych z identyfikatora i hasła innego użytkownika.
7. Każdy Użytkownik jest odpowiedzialny za zachowanie swojego hasła w tajemnicy.
8. Użytkownikowi nie wolno umieszczać haseł w widocznych miejscach ani też w żadnych automatycznych procesach logowania np.: skryptach, makrach.
9. Użytkownik powinien wprowadzać swoje hasła w taki sposób, aby uniemożliwić innym osobom poznanie tych haseł.
10. W przypadku, gdy Użytkownik podejrzewa, że hasło mogło zostać poznane przez osobę nieuprawnioną powinien niezwłocznie zmienić hasło na nowe.
11. Hasła powinny zostać tajemnicą także po utracie ich ważności.
12. Administrator Systemów Informatycznych jest odpowiedzialny za weryfikowanie listy użytkowników i usuwanie lub blokowanie zbędnych kont w systemach informatycznych.
13. Administrator Systemów Informatycznych powinien przeprowadzać przegląd uprawnień i autoryzacji nie rzadziej niż co 3 miesiące. Każdy przegląd powinien zostać odpowiednio udokumentowany.

Hasło Administratora Systemów Informatycznych

Hasło Administratora Systemów Informatycznych powinno być w należyty sposób przechowywane. Dostęp do niego powinni mieć wyłącznie Administrator Danych oraz Administrator Systemów Informatycznych. Konta o wysokich uprawnieniach powinny być wykorzystywane tylko w uzasadnionych sytuacjach i taki fakt powinien zostać udokumentowany.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA ORAZ ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU

Praca na stacjach roboczych

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu komputera i wprowadzeniu indywidualnego identyfikatora i hasła.
2. W pomieszczeniach gdzie przetwarzane są dane osobowe osoby postronne mogą przebywać tylko za zgodą i w obecności Użytkownika lub Inspektora Ochrony Danych Osobowych.
3. Na komputerach powinny być ustawione wygaszacze ekranu, które włączają się po 10 minutach od przerywania pracy przez Użytkownika. Wznowienie pracy powinno być możliwe po podaniu hasła.
4. W sytuacji, gdy użytkownik opuszcza stanowisko pracy, powinien wylogować się z systemu lub w inny sposób zablokować dostęp do komputera. Nie dopuszczalne jest pozostawienie komputera z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika.
5. Przesyłanie danych osobowych pocztą elektroniczną powinno być zabezpieczone poprzez szyfrowanie wiadomości.
6. Zakończenie pracy na komputerze możliwe jest po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary serwera i prawidłowym wylogowaniu się z systemu przez użytkownika i wyłączeniu komputera.
7. Przed opuszczeniem stanowiska pracy należy schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe oraz wszelkie inne dokumenty zawierające takie dane. Ponadto, należy zniszczyć w niszczarce zbędne dokumenty i wydruki.
8. Jeżeli to możliwe, pomieszczenie po zakończeniu pracy powinno zostać zamknięte na klucz.

Praca na komputerach przenośnych

1. Przy przetwarzaniu danych na komputerach przenośnych należy stosować te same procedury, które są używane przy pracy stacjach roboczych.
2. Użytkownicy korzystający z komputerów przenośnych powinni chronić je przed uszkodzeniami, kradzieżą oraz dostępem osób nieupoważnionych.
3. Wprowadza się zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy tych komputerów.
4. Praca na komputerze przenośnym możliwa jest tylko po wprowadzeniu indywidualnego identyfikatora i hasła Użytkownika.
5. Użytkownicy zmieniają hasła na komputerach przenośnych nie rzadziej niż co 30 dni.
6. Dyski w komputerach przenośnych powinny być szyfrowane, a dostęp do nich powinien być możliwy po podaniu hasła dostępu.
7. Użytkownikom komputerów przenośnych nie wolno samodzielnie modernizować sprzętu i oprogramowania. Wszelkie zmiany i aktualizacje powinny być dokonywane przez Administratora Systemów Informatycznych.

8. Wszelkie dokumenty zawierające dane osobowe, znajdujące się na stacjach roboczych, na koniec dnia pracy, muszą być usunięte z dysku.

PROCEDURA TWORZENIA KOPII ZAPASOWYCH

1. Wszelkie kopie w systemach informatycznych wykorzystujących technologię klient-serwer wykonuje się po stronie serwera.
2. Kopie bezpieczeństwa są sporządzane i przechowywane przez firmy zewnętrzne z zachowaniem koniecznych procedur upoważniających do przetwarzania danych osobowych. W tym celu niezbędne są następujące dokumenty:
 - a) Umowa powierzenia przetwarzania danych osobowych, zawarta między BP, a firmą zewnętrzną.
 - b) Imienne upoważnienie do przetwarzania danych osobowych.

Częstotliwość wykonywania kopii

Kopie zapasowe tworzone są przez firmy zewnętrzne z zachowaniem koniecznych procedur upoważniających do przetwarzania danych osobowych.

Przechowywanie kopii zapasowych

Kopie zapasowe przechowywane są przez firmy zewnętrzne z zachowaniem koniecznych procedur upoważniających do przetwarzania danych osobowych.

Testowanie kopii zapasowych

Dla celów weryfikacji poprawności wykonywania kopii zapasowych co najmniej raz na 6 tygodni poddaje się testowi kopię zapasową. Próba polega na testowym odtworzeniu danych i sprawdzeniu ich poprawności.

Likwidacja nośników zawierających kopie zapasowe

1. Nośniki z nieaktualnymi kopiami danych osobowych, będące poza wykazem cyklicznych kopii, powinno się likwidować. W przypadku nośników jednorazowych likwidacja polega na fizycznym zniszczeniu tych nośników w sposób uniemożliwiający odczytanie zawartych na nich danych. Nośniki wielokrotnego użytku takie jak taśmy, dyski twarde, płyty DVD-RW, CD-RW, Blu-ray-RW można wykorzystywać ponownie po dokładnym usunięciu i zamazaniu zawartości.
2. Uszkodzone nośniki wielokrotnego użytku należy zniszczyć fizycznie, np.: w specjalnej niszczarce.



PROCEDURA POSTĘPOWANIA NA WYPADEK WYSTĄPIENIA AWARII

Postępowanie w przypadku awarii jednostkowej

W razie wystąpienia awarii jednostkowej kierownik filii lub oddziału (lub osoba go zastępująca) zgłasza usterkę drogą elektroniczną (skrzynka e-mail: awaria@bppragapd.pl). Dalsze postępowanie uzależnione jest od charakteru problemu i pozostaje w gestii Działu Komputeryzacji i Edukacji Informatycznej. W tym wypadku obsługa czytelnika powinna być nadal realizowana dzięki zdublowanym stanowiskom obsługi.

Postępowanie w przypadku awarii zwykłej

- Systemu SOWA SQL – kierownik filii lub oddziału (lub osoba go zastępująca) zgłasza usterkę drogą elektroniczną (skrzynka e-mail: awaria@bppragapd.pl) do Działu Komputeryzacji i Edukacji Informatycznej, a następnie pracownik Działu przekazuje zgłoszenie do Administratora Systemu Bibliotecznego SOWA SQL, który ustala i usuwa przyczynę, która doprowadziła do awarii.
- Dostępu do Internetu w całej filii – kierownik filii lub oddziału (lub osoba go zastępująca) zgłasza usterkę drogą telefoniczną do Działu Komputeryzacji i Edukacji Informatycznej (pod numer telefonu: 22 671-04-51 wew. 116), a następnie pracownik Działu ustala i usuwa przyczynę, która doprowadziła do awarii.

W wypadku przedłużającej się awarii zwykłej obsługa czytelnika odbywa się w sposób następujący:

1. Kierownik filii lub oddziału umieszcza informację o awarii systemu w widocznym miejscu przy wejściu do placówki.
2. Administrator Systemów Informatycznych – umieszcza informację o awarii systemu na głównej stronie WWW oraz na stronie pracowniczej (intranet).
3. Zwroty książek przyjmowane są bez rejestracji.
4. Wypożyczenia notowane są w Rejestrze Wypożyczeń Awaryjnych, który zawiera datę, nazwisko, imię i numer czytelnika na podstawie Karty Czytelnika, numery inwentarzowe książek oraz podpis czytelnika (Załącznik nr 1).
5. Jednoczesne wypożyczenia są ograniczone do trzech egzemplarzy.
6. Zapisy nowych czytelników są wstrzymane.
7. Po ustaniu awarii wszystkie operacje z Rejestru Wypożyczeń Awaryjnych oraz zwroty książek zostają niezwłocznie wprowadzone do systemu SOWA SQL.

Postępowanie w przypadku awarii krytycznej

1. W razie wystąpienia awarii krytycznej systemu teleinformatycznego Administrator Systemów Informatycznych ustala przyczynę, która doprowadziła do awarii.
2. Po wykryciu usterki Administrator Systemów Informatycznych próbuje w jak najszybszy sposób przywrócić prawidłowe działanie systemu informatycznego. Jeżeli jest to konieczne,

zgłasza problem dostawcy Internetu, Administratorowi Systemu Bibliotecznego SOWA SQL, bądź firmie SOKRATES-Software.

3. Administrator Systemów Informatycznych informuje Inspektora Ochrony Danych Osobowych o zaistniałej sytuacji.
4. W wypadku przedłużającej się awarii krytycznej obsługa czytelnika odbywa się według zasad przyjętych przy powstaniu awarii zwykłej.

Zalecenia dalszego postępowania

1. W razie przedłużającej się awarii zwykłej lub krytycznej ponad 4 godziny, kierownik filii lub oddziału konsultuje się z instruktorem w celu ustalenia dalszego postępowania w zakresie obsługi czytelników.
2. Po ustaniu awarii krytycznej Administrator Systemów Informatycznych składa raport pisemny o zaistniałym zdarzeniu Dyrektorowi Biblioteki (zgodnie z „Polityką zarządzania ryzykiem w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga Południe m.st. Warszawy”, rozdział IX – „Incydenty”, §28 i §29).
3. Po ustaniu awarii zwykłej lub jednostkowej kierownik filii lub oddziału (lub osoba go zastępująca) składa raport pisemny o zaistniałym zdarzeniu pracownikowi zajmującemu się kontrolą zarządczą (zgodnie z „Polityką zarządzania ryzykiem w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga Południe m.st. Warszawy”, rozdział IX – „Incydenty”, §28 i §29). Informacja ta zostaje zachowana w dokumentacji kontroli zarządczej.
4. W przypadku stwierdzenia naruszenia ochrony danych osobowych, Administrator Systemów Informatycznych w porozumieniu z Inspektorem Ochrony Danych Osobowych działają zgodnie z zasadami przyjętymi w Bibliotece zawartymi w Instrukcji Bezpieczeństwa Informacji oraz w Instrukcji Przetwarzania Danych Osobowych.

PRZECHOWYWANIE ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI Z DANYMI OSOBOWYMI

1. Zbiory danych przechowywane są na serwerach obsługujących system informatyczny Administratora Danych. Dane, które są przetwarzane w pamięci stacji roboczych i komputerów przenośnych powinny być niezwłocznie umieszczane na serwerach w pomieszczeniach serwerowni.
2. Zabronione jest przetwarzanie danych osobowych na zewnętrznych nośnikach informacji.
3. Zbiory danych Systemu Bibliotecznego SOWA SQL, przechowywane są na serwerach hostingowych firmy SOKRATES-Software.

SPOSÓB ZABEZPIECZANIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓRE MOŻE UZYSKAĆ NIEUPRAWNIONY DOSTĘP DO DANYCH OSOBOWYCH

1. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez Administratora Systemów Informatycznych.

2. Oprogramowanie antywirusowe sprawuje ciągły nadzór nad pracą systemu i jego zasobami oraz serwerami, stacjami roboczymi oraz komputerami przenośnymi.
3. Administrator Systemów Informatycznych nie rzadziej niż raz na miesiąc przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach, stacjach roboczych i komputerach przenośnych.
4. Do obowiązków Administratora Systemów Informatycznych należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
5. Użytkownik niezwłocznie powiadamia Administratora Systemów Informatycznych o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
6. Użytkownicy mogą korzystać z zewnętrznych nośników danych, po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.
7. Zewnętrzne nośniki danych służą tylko w celach służbowych na terenie placówek BP lub na terenie podmiotów współpracujących z BP.
8. Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych i komputerach przenośnych, sieć wewnętrzna jest chroniona centralnym urządzeniem sprzętowym z wbudowanym Firewall.

KONTROLA NAD WPROWADZENIEM, PRZETWARZANIEM I UDOSTĘPNIANIEM DANYCH OSOBOWYCH

1. System informatyczny służący do przetwarzania danych osobowych powinien zapewniać każdej osobie, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
2. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione, chyba że dane pochodzą z jawnego zbioru danych osobowych.
3. W przypadku zgłoszenia sprzeciwu, o którym mowa w art. 21 ust. 1 RODO, wobec przetwarzania danych osobowych system powinien zapewniać odnotowywanie tej informacji.
4. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne.

PROCEDURY WYKONYWANIA KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Konserwacji systemu dokonuje Administrator Systemów Informatycznych lub osoby przez niego wyznaczone doraźnie.
2. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje Inspektor Ochrony Danych Osobowych i Administrator Systemów Informatycznych, Administrator Systemu Bibliotecznego SOWA SQL, w przypadku wykrycia błędu.

NAPRAWY URZĄDZEŃ KOMPUTEROWYCH Z DANymi OSOBOWymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych przeprowadzane są pod nadzorem Administratora Systemu.
2. Naprawy i zmiany w systemie informatycznym Administratora Danych Osobowych przeprowadzane przez serwisanta prowadzone są pod nadzorem Administratora Systemów Informatycznych w siedzibie Administratora Danych (jeśli to możliwe) lub poza siedzibą Administratora Danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umowy powierzenia przetwarzania danych osobowych.
3. Jeśli nośnik danych: dysk, płyta lub inny zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć fizycznie, np.: w specjalnej niszczarce.

WYMAGANIA DOTYCZĄCE SPRZĘTU I OPROGRAMOWANIA

1. Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
2. Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty Administratora Systemów Informatycznych.
3. Przed zainstalowaniem nowego oprogramowania Administrator Systemów Informatycznych lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
4. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.
5. Serwer systemu przetwarzającego dane osobowe powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak aby przed ostatecznym zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.

6. Wdrażanie aplikacji i oprogramowania eksploatowanych systemów powinno być poprzedzone wyczerpującymi, pozytywnymi i udokumentowanymi testami przeprowadzonymi w wydzielonym w tym celu środowisku.
7. Należy przechowywać wszystkie poprzednie wersje oprogramowania jako środek utrzymania ciągłości działania.
8. Należy zapewnić rejestrowanie wszystkich błędów, związanych z problemami przetwarzania danych osobowych, zgłaszanych przez użytkowników lub programy systemowe.
9. Należy chronić informacje zawarte w dziennikach zdarzeń systemów przed manipulacją i nieautoryzowanym dostępem.
10. Należy zapewnić, aby porty i usługi, które nie są wykorzystywane były zablokowane.

HARMONOGRAM CYKLICZNEGO BADANIA PODATNOŚCI SYSTEMÓW IT

Celem opracowania harmonogramu badania podatności systemów IT (Załącznik nr 2), jest zaplanowanie działań, a co za tym idzie zaplanowanie zasobów (ludzkich, sprzętowych) w celu podniesienia sprawności systemów IT w Bibliotece. Terminy wykonania poszczególnych zadań mogą być przesuwane ze względów organizacyjnych.

Zakres badań

Badanie podatności systemów IT zostanie podzielone na:

1. Testy infrastruktury IT pozwolą na zbadanie takich podatności jak:
 - Nieaktualne wersje systemów operacyjnych i aplikacji sieciowych (serwery: WWW, aplikacyjne, baz danych, pocztowe, DNS, SSH i inne).
 - Obecność niepotrzebnych (z punktu widzenia najlepszych praktyk bezpieczeństwa) usług sieciowych.
 - Nieprawidłowa konfiguracja usług sieciowych.
 - Użycie domyślnych lub słabych haseł.
 - Znane podatności publikowane przez producentów oprogramowania/sprzętu oraz przez niezależnych badaczy.
 - Inne zidentyfikowane słabe punkty systemów, będące źródłem zagrożeń i zwiększające ryzyko awarii.
2. Testy bezpieczeństwa aplikacji:
 - Uwierzytelnianie użytkowników w systemie.
 - Mechanizmy autoryzacji użytkowników.
 - Mechanizm zarządzania użytkownikami.
 - Mechanizmy walidacji danych wejściowych i wyjściowych (input/output).
 - Mechanizmy obsługi błędów i wyjątków.
 - Funkcjonalność i funkcje administracyjne systemu.
 - Inne zidentyfikowane w trakcie działania testu.
3. Przegląd Instrukcji Bezpieczeństwa Informacji.



Przebieg badań

Badanie wewnętrzne będzie wykonywane w cyklach rocznych. Zadania zostaną wykonane w następujących etapach:

1. Testy.
2. Raport z testów.
3. Propozycje działań korygujących.
4. Wprowadzenie działań korygujących.

POSTANOWIENIA KOŃCOWE

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Każda osoba upoważniona do przetwarzania danych osobowych jest zapoznawana przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz składa pisemne oświadczenie, potwierdzające znajomość jej treści.
3. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.

SPIS ZAŁĄCZNIKÓW

1. Załącznik nr 1 - Rejestr Wypożyczeń Awaryjnych
2. Załącznik nr 2 - Harmonogram cyklicznego badania podatności systemów IT
3. Załącznik nr 3 – wykaz pomieszczeń, w których przetwarzane są dane osobowe



[illegible]

17

Załącznik nr 3

Wykaz budynków gdzie przetwarzane są dane osobowe:

1. Biblioteka dla Dzieci i Młodzieży Nr 2 – Witoszyńskiego 2
2. Biblioteka dla Dzieci i Młodzieży Nr 16 – Walewska 7a
3. Biblioteka dla Dzieci i Młodzieży Nr 42 – Biskupia 50
4. Biblioteka dla Dzieci i Młodzieży Nr 45 – Meksykańska 3
5. Biblioteka dla Dzieci i Młodzieży Nr 47 – Paca 46
6. Biblioteka dla Dzieci i Młodzieży Nr 55 – Egipska 7
7. Biblioteka dla Dzieci i Młodzieży Nr 67 – Abrahama 10
8. Wypożyczalnia dla Dorosłych i Młodzieży Nr 3 – Waszyngtona 2b
9. Wypożyczalnia dla Dorosłych i Młodzieży Nr 18 – Grochowska 118
10. Wypożyczalnia dla Dorosłych i Młodzieży Nr 19 – Witoszyńskiego 2
11. Wypożyczalnia dla Dorosłych i Młodzieży Nr 24 – Grochowska 279
12. Wypożyczalnia dla Dorosłych i Młodzieży Nr 40 – Paca 46
13. Wypożyczalnia dla Dorosłych i Młodzieży Nr 44 – Grochowska 333a
14. Wypożyczalnia dla Dorosłych i Młodzieży Nr 62 – Egipska 7
15. Wypożyczalnia dla Dorosłych i Młodzieży Nr 66 – Angorska 14
16. Wypożyczalnia dla Dorosłych i Młodzieży Nr 78 – Majdańska 5
17. Wypożyczalnia dla Dorosłych i Młodzieży Nr 89 – Grochowska 202
18. Wypożyczalnia dla Dorosłych i Młodzieży Nr 90 – Rozłucka 11a
19. Wypożyczalnia dla Dorosłych i Młodzieży Nr 92 – Biskupia 50
20. Wypożyczalnia dla Dorosłych i Młodzieży Nr 94 – Meksykańska 3
21. Wypożyczalnia dla Dorosłych i Młodzieży Nr 100 – Zwycięzców 46
22. Wypożyczalnia dla Dorosłych i Młodzieży Nr 110 – Abrahama 10
23. Wypożyczalnia Zbiorów Obcojęzycznych – Meissnera 5
24. Wypożyczalnia Książki Mówionej i Multimedialnych – Meissnera 5
25. Czytelnia Naukowa Nr V – Meissnera 5
26. Dział Komputeryzacji i Edukacji Informatycznej – Meissnera 5

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając w imieniu Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy z siedzibą w Warszawie 03-982, przy ul. Meissnera 5 (dalej „BP”), jako Inspektor Ochrony Danych Osobowych, na mocy pełnomocnictwa do nadawania upoważnień udzielonego przez Administratora Danych, na podstawie Polityki Bezpieczeństwa Informacji obowiązującej w BP oraz zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) **upoważniam:**

Imię i nazwisko upoważnianej osoby	
Zbiory danych objęte zakresem upoważnienia	
Identyfikator	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. i obowiązującymi w BP wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy lub odpowiedzialności cywilnej.

Upoważnienie jest ważne do czasu zakończenia stosunku pracy, stosunku cywilnoprawnego lub odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się – w zakresie wynikającym z przydzielonych zadań – z obowiązującymi w odniesieniu do ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w BP (w szczególności z Dokumentacją ochrony danych osobowych). Przyjmuję do wiadomości zawarte w nich obowiązki dotyczące ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub współpracy.

Data i podpis osoby upoważnionej

chaf



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

Warszawa, dnia

ZAŚWIADCZENIE

Pan/i

.....

odbył/a szkolenie wewnętrzne w zakresie

Ochrona danych osobowych w bibliotece

na poziomie podstawowym

(na podstawie Polityki Bezpieczeństwa Informacji obowiązującej w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy, Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. Dz.U. 2018 poz. 1000)

Szkolenie przeprowadził Inspektor Ochrony Danych Osobowych w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy

.....
Podpis i pieczęć IODO

Chaf

**Wykaz zbiorów danych osobowych, których Administratorem Danych jest Biblioteka Publiczna
im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy, zwana dalej Biblioteką**

L.p.	Nazwa Zbioru	Nazwa programu
1.	Czytelnicy	Sowa SQL
2.	Rodzice i opiekunowie prawni osób małoletnich	Sowa SQL
3.	Pracownicy	Raks SQL, Microsoft Office, Płatnik, postać tradycyjna
4.	Współpracownicy }	Raks SQL, Microsoft Office, Płatnik, postać tradycyjna
5.	Kandydaci do pracy	Microsoft Office

Chap

*Koloriem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO

1	2	3	4	5	6	7	8	10	11	12	13	
LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy)	Kategorie odbiorców (innych niż podmiot przetwarzający)	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)
		Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g
1.	Rekrutacja pracowników	Dyrektor Biblioteki	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych, adres e-mail, nr telefonu, data urodzenia, zainteresowania	Zgoda osób, których dana dotyczy, [art. 23.1. UODO z 29 sierpnia 1997 (Dz. U. 2016 poz. 922)] • Przepis prawa. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22 ¹ § 1.	Kandydaci do pracy	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Dokumentacja papierowa.	zamykane w szafach w pomieszczeniu Dyrektora Biblioteki, pokój z kodowanym dostępem w strefie ograniczonego dostępu, dostęp tylko dla uprawnionych osób
2.	Prowadzenie rejestru pracowników, akt ewidencyjnych i ewidencji czasu ich pracy	Kadry	Prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy	Pracownicy (receptjonisci, sprzątaczk, pracownicy gospodarczy), administracyjni oraz bibliotekarze	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem Pracy	• Umowa o pracę. • Przepis prawa. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22 ¹ w związku z art. 94 pkt 9a i 9b	Pracownik	50 lat [art. 51u ust 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy	ZUS, Urząd Skarbowy, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	System RAKS, Dokumentacja papierowa.	Zamykane metalowe szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób, w strefie ograniczonego dostępu. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób.

Ciały

3.	Zgłoszenie pracowników i członków ich rodzin do ZUS, ich aktualizacja i przekazywanie danych o zwolnieniach.	Kadry	Zgłoszenia pracowników i członków jego rodziny do ZUS, ich aktualizacja oraz przekazywanie informacji o zwolnieniach.	Pracownicy obsługi (recepjoniści, sprzątaczkę, pracownicy gospodarczy), administracyjni oraz bibliotekarze	Dane Identyfikacyjne, dane adresowe, dane o Oddziale NFZ oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - 2017 r., poz. 1778 t.i.) zgłoszenia ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA - zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny	• Przepis prawa. Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1383)	Pracownik	50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. z 2017 r., poz. 1383)]	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	System PUE, Płatnik. Dokumentacja papierowa.	Zamykane metalowe szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób, w szafie ograniczonego dostępu. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób. Posiadanie podpisu elektronicznego przez osobę upoważnioną.
4.	Prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS	Kadry	Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS	Pracownicy obsługi (recepjoniści, sprzątaczkę, pracownicy gospodarczy), administracyjni oraz bibliotekarze	Dane Identyfikacyjne, dane adresowe, dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach (składki związkowe, zaliczka komornicze itp.) numery kont dla przelewów bankowych pracowników	Umowa o pracę. Przepis prawa. • Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) Dział III - Wynagrodzenia; Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.i.) - art. 1, 6 oraz 6a;	Pracownik	50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. z 2017 r., poz. 1383)]	Nie dotyczy	Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe,	Dyski sieciowe, wiadomości e-mail do związku "Solidarność" i do Biblioteki na ul. Koszykowej (zawiera imię i nazwisko, wysokość potrącenia); Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.
5.	zgłoszenie pracowników do ubezpieczenia zbrojowego, wykonywanie operatywnych świadczeń	Księgowość	zgłoszenie pracowników do ubezpieczenia zbrojowego	Pracownicy	imię, nazwisko, data i miejsce urodzenia, nr telefonu, nr PESEL, imiona rodziców, dane osób uposażonych, dokumentacja medyczna, akty zgonu	umowa z ubezpieczycielem	Pracownicy		PZU S.A.	System Eru PZU	Elektroniczny system rekrutacji. Dokumentacja papierowa.	upoważnienie ubezpieczyciela, dostęp tylko dla upoważnionych osób, upoważnienie ADO, kontrola dostępu do systemu informatycznego, pomieszczenie kodowane

Chap3

6	księgowanie plac	księgowość	księgowanie plac	Pracownicy	imię i nazwisko, nr rachunku bankowego, adres zamieszkania		Pracownicy	zakończenie umowy cywilno-prawnej			System RAKS	dostęp tylko dla upoważnionych osób, upoważnienie ADO, kontrola dostępu do systemu informatycznego, niepowtarzalny kod dostępu, pomieszczenie kodowane
7	operacje kasowe i przelewy bankowe dokonywane limitnie	księgowość	wypłacanie i wypłacanie należności w formie gotówkowej i elektronicznej	Kontrahenci i pracownicy	imię, nazwisko, adres, nr rachunku bankowego	ustawa o finansach publicznych (Dz.U. 2009 nr 157 poz. 1240)	Kontrahenci i pracownicy	ustanie stosunku pracy/ 2 lata po ustaniu aktywności kontrahenta			System RAKS, system BiznesPro	karty do czytników, własny login i hasło, polecenie dostępności, dostęp tylko dla upoważnionych osób, pomieszczenie kodowane
8	naliczanie i wypłacanie świadczeń socjalnych	Zakładowa Komisja Świadczeń Socjalnych, przedstawiciel pracodawcy, "Solidarność" i "Związek Zawodowy Bibliotekarzy Polskich i Pracowników Biblioteki"	naliczanie i wypłacanie świadczeń socjalnych	Pracownicy i emeryci, członkowie ich rodzin	imię, nazwisko, adres, nr PESEL, data urodzenia, nr telefonu, dochody na osobę w rodzinie, sytuacje trudne, oświadczenie o dochodach na osobę w rodzinie, imię, nazwisko data urodzenia dziecka, wysokość przyznanego świadczenia, dane osób zgłoszonych do wyjazdów w ramach działalności socjalnej	umowa o pracę z pracownikiem umowa o wysokosć udzielonej pożyczki	Pracownicy, emeryci	5 lat	biuro podróży FOKUS - dane do ubezpieczenia: imię, nazwisko, data urodzenia		dyski sieciowe	dokumentacja papierowa zamykana w szafach na klucz upoważnienia dla pracowników, kontrola dostępu do systemu informatycznego, pomieszczenie kodowane

Chapf

ZGODA NA PUBLIKACJĘ WIZERUNKU

Wyrażam zgodę na zamieszczenie przez **Bibliotekę Publiczną im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy, ul. Meissnera 5 w Warszawie** mojego wizerunku / wizerunku mojego dziecka, utrwalonego podczas przeprowadzonego szkolenia/spotkania, którego byłem/am/o uczestnikiem, na:

- ☐ stronie Biblioteki **www.bppragapd.pl**
- ☐ wydawnictwie „**BIBLIOTEKON**”
- ☐ profilu Biblioteki na portalu społecznościowym „**Facebook**”
- ☐ wystawach i prezentacjach Biblioteki

w celach promocyjnych oraz sprawozdawczych.

Zostałem/am poinformowany/a, iż wyrażenie zgody jest dobrowolne. Przysługuje mi prawo dostępu do treści moich danych oraz ich poprawienia.

Warszawa,.....
(miejscowość, data)

.....
(czytelny podpis osoby wyrażającej zgodę)





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

KLAUZULA OBOWIĄZKU INFORMACYJNEGO W STOSUNKU DO CZYTELNIKA

Zgodnie z art. 13 ust. 1 i ust. 2 RODO - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (dalej RODO) i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), informujemy:

- | |
|---|
| 1. Administratorem Danych Osobowych jest Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m.st. Warszawy
dane kontaktowe:
e-mail: dyrekcja@bppragapd.pl
tel. 22 671-05-11 |
| 2. Biblioteka wyznaczyła Inspektora Ochrony Danych Osobowych
dane kontaktowe
e-mail: iodo@bppragapd.pl
tel. 22 671-05-41 wew. 104 |
| 3. <u>Cel przetwarzania danych oraz podstawa prawna:</u>
a) dane identyfikujące Czytelnika oraz dotyczące korzystania przez Czytelnika z usług Biblioteki, są przetwarzane w związku z wykonywaniem zadań w interesie publicznym (Ustawa o Bibliotekach, art. 6 ust. 1 lit.e RODO) i służą do następujących celów:
- udostępniania i wypożyczania materiałów bibliotecznych,
- dokumentowania prowadzonej działalności oraz informowania o niej, co obejmuje również przetwarzanie w celach archiwalnych w interesie publicznym.
b) dane identyfikujące Czytelnika i jego status społeczno-zawodowy, dane dotyczące jego zobowiązań wobec Biblioteki oraz sposobu korzystania z Internetu lub sieci Wi-Fi Biblioteki (jeśli Czytelnik korzysta z tych usług), w tym dane identyfikujące komputer Czytelnika, są przetwarzane w związku z obowiązkami prawnymi ciążącymi na Bibliotece (ustawa o finansach publicznych, ustawa o statystyce publicznej, ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, art. 6 ust. 1 lit.c RODO) i służą do następujących celów:
- dochodzenia ewentualnych roszczeń prawnych,
- opracowywania statystyk dotyczących działalności Biblioteki,
- zapewnienia bezpieczeństwa sieci i systemów informatycznych Biblioteki.
c) adres poczty elektronicznej oraz numer telefonu Czytelnika mogą być przetwarzane na podstawie zgody (art. 6 ust. 1 lit.a RODO) w następujących celach:
- powiadamiania o terminach zwrotów materiałów bibliotecznych, powiadamiania o możliwości odbioru zamówionych materiałów oraz prowadzenia korespondencji o podobnym charak- |

terze, prowadzenia korespondencji w celu dochodzenia roszczeń, przekazywania informacji o działalności Biblioteki.

4. Kategorie odbiorców danych:

- a) podmiot utrzymujący na swoich serwerach system biblioteczny oraz inne podmioty, którym powierza się przetwarzanie danych, z zastrzeżeniem, że takie podmioty nie nabywają praw do samodzielnego decydowania o przetwarzaniu tych danych, a jedynie wykonują polecenia Biblioteki.

5. Okres przechowywania danych wynosi:

- a) dla danych przetwarzanych w celu udostępniania i wypożyczania materiałów bibliotecznych, komunikowania się z Czytelnikiem oraz opracowywania statystyk – nie więcej niż 5 lat od końca roku, w którym Czytelnik ostatni raz korzystał z usług Biblioteki, pod warunkiem, że nie jest wobec niej zadłużony,
- b) dla danych przetwarzanych w celu dochodzenia ewentualnych roszczeń prawnych – do czasu przedawnienia roszczeń lub zakończenia postępowania związanego z dochodzeniem roszczenia,
- c) dla danych przetwarzanych w celu dokumentowania prowadzonej działalności oraz informowania o niej – nie więcej niż 5 lat od dnia dokumentowanego wydarzenia, chyba że dane są przetwarzane w celach archiwalnych w interesie publicznym,
- d) dla danych przetwarzanych w celu zapewnienia bezpieczeństwa sieci i systemów informacyjnych Biblioteki – nie więcej niż 5 lat od dnia zarejestrowania,
- e) dla danych przetwarzanych na podstawie zgody Czytelnika – do czasu wycofania tej zgody.

6. Przysługujące Czytelnikowi prawa, w tym prawo do sprzeciwu:

- a) osobie, której dane dotyczą, przysługuje prawo żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec przetwarzania oraz prawo przenoszenia danych,
- b) dopuszczalność korzystania z poszczególnych praw zależy od podstawy prawnej konkretnego przetwarzania,
- c) zgoda może być w dowolnym momencie wycofana, bez wpływu na zgodność z prawem przetwarzania, którego dokonano przed wycofaniem,
- d) osoba, której dane dotyczą, ma prawo wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych.

7. Informacja o wymogu dobrowolności podania danych oraz konsekwencjach ich niepodania:

- a) podanie danych osobowych jest dobrowolne. Odmowa podania danych skutkuje odmową zapisu do Biblioteki lub brakiem możliwości korzystania z jej usług.



WZÓR KARTY ZOBOWIĄZANIA CZYTELNIKA

Karta zobowiązania

Legitymacja:	Nazwisko i imię:	Dodatkowe dane:	
Data zapisu:	Data ważności:	Limit konta:	
PESEL:	Data urodzenia:	Płeć:	
Adres do korespondencji:	Dokument tożsamości:	Grupa statystyczna:	
Powiadomienia SMS:	*Adres e-mail:	*Dodatkowy adres e-mail:	*Telefon kontaktowy:
*Osoba upoważniona:		*Telefon:	

Oświadczam, że podane przeze mnie dane są prawdziwe.

Oświadczam, że zasady korzystania z zasobów Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m. st. Warszawy, zawarte w Regulaminie Biblioteki, są mi znane i będę ich przestrzegać.

Oświadczam, że zapoznałem się z Klauzulą informacyjną dotyczącą przetwarzania danych osobowych w Bibliotece.

Na podstawie art. 6 ust.1 lit a. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), wyrażam zgodę na przetwarzanie moich danych osobowych przez Bibliotekę Publiczną im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m. st. Warszawy, takich jak:

- adres e-mail,
- telefon kontaktowy,
- osoba upoważniona.

DATA _____
Podpis Czytelnika

*pola oznaczone gwiazdką nie są obowiązkowe, jednakże ich podanie usprawni kontakt Biblioteki z Czytelnikiem. Podanie pozostałych danych jest niezbędne do utworzenia konta czytelnika i korzystania z zasobów bibliotecznych.



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

WZÓR KARTY ZOBOWIĄZANIA CZYTELNIKA

Karta zobowiązania opiekuna prawnego

Legitymacja:		Nazwisko i imię:		Dodatkowe dane:	
Data zapisu:		Data ważności:		Limit konta:	
PESEL:		Data urodzenia:		Płeć:	
Adres do korespondencji:		Dokument tożsamości:		Grupa statystyczna:	
Powiadomienia SMS:	*Adres e-mail:		*Dodatkowy adres e-mail:		*Telefon kontaktowy:
Nazwisko i imię opiekuna prawnego:		Pokrewieństwo:		PESEL:	
Adres do korespondencji opiekuna:		Kontakt z opiekunem:		Dokument tożsamości opiekuna:	
*Osoba upoważniona:			*Telefon:		

Oświadczam, że podane przeze mnie dane są prawdziwe.

Oświadczam, że zasady korzystania z zasobów Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m. st. Warszawy, zawarte w Regulaminie Biblioteki, są mi znane i będę ich przestrzegać.

Oświadczam, że zapoznałem się z Klauzulą informacyjną dotyczącą przetwarzania danych osobowych w Bibliotece.

Na podstawie art. 6 ust.1 lit a. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), wyrażam zgodę na przetwarzanie moich danych osobowych przez Bibliotekę Publiczną im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m. st. Warszawy, takich jak:

- adres e-mail,
- telefon kontaktowy,
- osoba upoważniona.

DATA _____

Podpis opiekuna prawnego

**pola oznaczone gwiazdką nie są obowiązkowe, jednakże ich podanie usprawni kontakt Biblioteki z Czytelnikiem/opiekunem prawnym Czytelnika. Podanie pozostałych danych jest niezbędne do utworzenia konta czytelnika i korzystania z zasobów bibliotecznych.*

Biblioteka Publiczna im. Zygmunta Jana Rumla
w Dzielnicy Praga-Południe m. st. Warszawy
ul. Meissnera 5, 03-982 Warszawa

**Wniosek o usunięcie danych osobowych z bazy Biblioteki Publicznej im. Z.J. Rumla w Dzielnicy
Praga-Południe m. st. Warszawy**

Nr karty bibliotecznej:.....

Zgodnie z art. 17.1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - RODO, ja niżej podpisany/a wnoszę o zaprzestanie przetwarzania moich danych osobowych oraz całkowite usunięcie danych z bazy Biblioteki Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m. st. Warszawy.

Warszawa

Miejscowość i data

.....

Podpis

POTWIERDZENIE

Biblioteka Publiczna im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m. st. Warszawy, potwierdza, że zgodnie z Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku, na wniosek **Pana/Pani**.....

Nr karty bibliotecznej:.....

z dniem.....

zaprzestaje przetwarzać dane osobowe Wnioskodawcy oraz całkowicie usuwa te dane z bazy w Bibliotece Publicznej im. Zygmunta Jana Rumla w Dzielnicy Praga-Południe m. st. Warszawy, z zastrzeżeniem, iż dane nie zostaną usunięte w sytuacji dochodzenia roszczeń przeciwko Pani/Panu związanych z korzystaniem ze zbiorów Biblioteki .

Warszawa

Miejscowość i data

.....

Podpis



WZÓR: EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nazwisko i imię	Login użytkownika w systemie informatycznym	Nazwa zbioru	Data nadania	Data zmiany	Data odwołania	Zakres upoważnienia (bez ograniczeń/ podgląd danych/ zmiana danych/ usuwanie danych)	Nazwa systemu, w którym przetwarzane są dane

Raport z naruszenia bezpieczeństwa danych osobowych

IODO Sporządzający raport:

Imię i nazwisko:

Nr telefonu:

1. Miejsce, czas i data naruszenia ochrony danych osobowych (dział, pokój, godzina):

.....

2. Lokalizacja zdarzenia (numer pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

3. Rodzaj naruszenia i okoliczności towarzyszące naruszeniu:

.....

4. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):

.....

5. Kategorie danych, które zostały lub mogły zostać ujawnione:

.....

6. Przybliżona liczba osób, których dane dotyczą, oraz kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie:

.....

7. Możliwe konsekwencje naruszenia bezpieczeństwa danych osobowych:

.....

8. Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków:

.....

(podpis pracownika)

(data i podpis inspektora ochrony danych)

Chay

WZÓR: Rejestr naruszeń ochrony danych osobowych

Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorcemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

Ciały