TOM 3

STANDARDY KONTROLI ZARZĄDCZEJ
MUZEUM MIEJSKIEGO W ŻORACH

MUZE.ON

INFORMACJA I KOMUNIKACJA

MUZEUM MIEJSKIEGO W ŻORACH

2000 – 2019

Standardy kontroli zarządczej Muzeum Miejskiego w Żorach

TOM III

KOMUNIKACJA I INFORMACJA
MUZEUM MIEJSKIEGO W ŻORACH

Opracowanie: Katarzyna Podyma
Jacek Struczyk
Marta Szafraniec

Żory 2021

SPIS TREŚCI

POLITYKA KOMUNIKACJI

KOMUNIKACJA

1. Komunikacja w Muzeum Miejskim w Żorach (dalej: Muzeum) obejmuje:
    - informację operacyjną,
    - systemy informacji tradycyjnej lub skomputeryzowanej,
    - komunikację wewnętrzną,
    - komunikację zewnętrzną,
    - nieformalną wymianę informacji.

2. Zasady komunikacji w Muzeum:
    - metoda twarzą w twarz – naczelna metoda komunikacji,
    - wyjaśnienie zasad – zapoznanie z zasadami efektywnej komunikacji i wspólne opracowanie schematu przekazywania informacji,
    - określenie i ogłoszenie pozytywnych zmian – zmiany będące rezultatem właściwej komunikacji,
    - koordynowanie czasu komunikacji w celu uniknięcia demoralizujących plotek rozsiewanych przed formalnym oświadczeniem,
    - brak spekulacji – zmniejszenia niepewności,
    - zapewnianie wystarczającej ilości czasu na wypowiedź – swoboda wyrażania opinii,
    - komunikowanie się z zespołem w sposób jasny, uczciwy i konsekwentny – nieunikanie drażliwych tematów, stawianie wszystkich problemów otwarcie, przekazywanie informacji maksymalnie uproszczone i łatwe do zapamiętania,
    - tworzenie nowych nośników komunikacji.

3. Reguły komunikacji w Muzeum Miejskim:
    - Miej jasność co do tego, kim jest odbiorca. Jaki jest stan umysłu odbiorcy? Co odczuwa w danej sytuacji?
    - Znaj własny cel. Co chcesz uzyskać poprzez przekazanie komunikatu?
    - Przeanalizuj klimat. Czego będzie potrzeba, żeby pomóc odbiorcy odprężyć się i otworzyć się na komunikat?
    - Komunikuj się przy użyciu słów i terminów znanych drugiej osobie. Posługuj się przykładami i ilustracjami ze świata odbiorcy. Czy nie należałoby wyjaśnić niektórych myśli?

- Przeanalizuj w myśli komunikat, zanim go wypowiesz. Pomyśl o komunikacie z punktu widzenia odbiorcy.
- Jeżeli odnosisz wrażenie, że odbiorca cię nie rozumie, wyjaśnij komunikat. Zadawaj pytania. Jeżeli jest potrzebne powtórzenie komunikatu, spróbuj użyć innych słów i przykładów.
- Jeżeli odpowiedź sprawia wrażenie krytycznej, nie reaguj defensywnie. Staraj się zrozumieć, co odbiorca myśli. Dlaczego zareagował negatywnie? Być może źle zrozumiał twój komunikat. Zadaj pytania wyjaśniające.

A. BIEŻĄCA KOMUNIKACJA

Komunikacja zapewnia dyrektorowi oraz pracownikom otrzymanie w odpowiedniej formie i czasie właściwych i rzetelnych informacji potrzebnych im do wypełniania obowiązków, w szczególności wynikających z przyjętych standardów kontroli zarządczej.

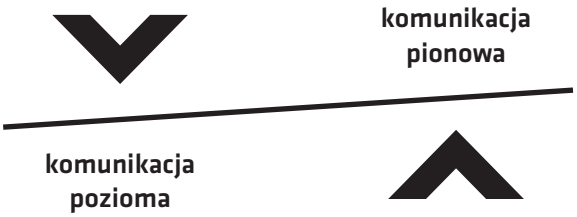
B. KOMUNIKACJA WEWNĘTRZNA

Komunikacja wewnętrzna jest jednym z głównych elementów kultury organizacji pracy Muzeum. Jest także podstawową funkcją tak zwanego wewnętrznego PR-u (public relations).

Ogół działań public relations obejmuje nie tylko kontakty z otoczeniem zewnętrznym i kreowaniem zewnętrznego wizerunku, ale także kontakt Muzeum z pracownikami oraz komunikację między samymi pracownikami.
Działania public relations związane z komunikacją w Muzeum obejmują budowę tzw. wizerunku wewnętrznego Muzeum, który jest nie mniej ważny od wizerunku firmy w otoczeniu zewnętrznym.

Komunikacja wewnętrzna obejmuje kanały kontaktu między poszczególnymi komórkami organizacyjnymi Muzeum Miejskiego.

MODEL KOMUNIKACJI WEWNĘTRZNEJ



KOMUNIKACJA POZIOMA

KOMUNIKACJA PIONOWA

Kanały komunikacyjne umożliwiające międzyszczeblowy przepływ informacji:

- kalendarz Google,
- Dropbox,
- tablica ogłoszeń,
- szkolenia i konferencje,
- ankiety.

Za pomocą wymienionych kanałów informacyjnych pracownicy są informowani o:

- wszystkich bieżących wydarzeniach związanych z pracą Muzeum,
- planowanych zmianach i wdrożeniach,
- ogólnej polityce Muzeum,
- oraz strategii rozwoju.

Narzędzia komunikacji służą uporządkowaniu relacji oraz podniesieniu świadomości zachodzących procesów. Kanały komunikacyjne są również wykorzystywane do motywowania pracowników.

SCHEMAT KOMUNIKACJI WEWNĘTRZNEJ MUZEUM MIEJSKIEGO

Komunikacja wewnętrzna regulowana jest poprzez próby wdrożeniowe socjologiczno-architektoniczne. Zmiany są wprowadzane pod wpływem analizy zaistniałych przypadków newralgicznych, których stara struktura nie była w stanie udźwignąć.

C. KOMUNIKACJA ZEWNĘTRZNA

MODEL KOMUNIKACJI ZEWNĘTRZNEJ

Podstawą wizerunku Muzeum jest współpraca z organizatorem, społeczeństwem i organizacjami pozarządowymi, która stwarza możliwości odpowiednich relacji ze wszystkimi interesariuszami, budując wizerunek Muzeum „społecznie odpowiedzialnego".

Wizerunek Muzeum budowany jest przede wszystkim za pomocą:

- działań bezpośrednich własnych,
- współorganizacji zadań,
- współpracy instytucjonalnej,
- strony internetowej,
- portali społecznościowych / „social mediów",
- Biuletynu Informacji Publicznej.

Na wizerunek Muzeum w komunikacji zewnętrznej wpływają:

- znak firmowy i jego barwy,
- rodzaj prowadzonej działalności,
- wszystkie materiały, które wychodzą z Muzeum na zewnątrz,
- zachowanie pracowników i wypowiadane przez nich opinie o Muzeum,
- zasady współpracy z klientami,
- sposób traktowania klientów,
- bezpośrednie rozmowy,
- spotkania grupowe,
- konferencje prasowe,
- informacje przekazywane prasie w formie notatek prasowych,
- odpowiadanie na pytania dziennikarzy,
- reklamę w mediach,
- wszelkiego rodzaju wydawnictwa reklamowe,
- wysyłanie listów,
- stronę internetową spójną z identyfikacją wizualną,
- kontakt drogą elektroniczną.

Podstawą budowania komunikacji zewnętrznej Muzeum jest spójność i czytelność dla odbiorców.

Wizerunek Muzeum budowany jest poprzez starannie dobraną formę przekazu informacji. Poprzez stały monitoring rynku, obserwowanie zachodzących na nim zmian i rozpoznanie potrzeb odbiorców wprowadzane są zmiany służące nowoczesnemu i spójnemu wizerunkowi.

Za wizerunek odpowiadają wszyscy pracownicy Muzeum, a w szczególności zespół promocji, który tworzy i odpowiada za realizację spójnej i nowoczesnej polityki PR, reklamy i marketingu.

Polityka PR, reklamy i marketingu jest elementem całościowej polityki Muzeum. Jest w trybie ciągłym poddawana monitoringowi, analizie i ewaluacji.

POLITYKA OCHRONY DANYCH OSOBOWYCH

1. WSTĘP

1.1 INFORMACJE OGÓLNE

1. Niniejsza Polityka ochrony danych osobowych (dalej: Polityka) wdrażana jest przez Muzeum Miejskie w Żorach (ul. Muzealna 1/2, 44-240 Żory), zwanym dalej Administratorem Danych Osobowych (ADO). Jej aktualizacja ma miejsce w związku z wejściem w życie 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, dalej zwane „RODO".
2. Głównym celem wprowadzenia Polityki jest zapewnienie bezpieczeństwa przetwarzanych danych w strukturze podległej Administratorowi Danych Osobowych oraz dostosowanie organizacji do standardów RODO, ustawy o ochronie danych osobowych z 2018 r. oraz aktów wykonawczych.
3. Polityka została opracowana w oparciu o wytyczne zawarte w następujących aktach prawnych:
   a) 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,
   b) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 z późn. zm.).

1.2 CEL DOKUMENTU

Niniejsza Polityka ma na celu zidentyfikowanie zagrożeń, przyczyn i skutków naruszeń ochrony danych osobowych, a także dostarczenie narzędzi rejestracji i wzorców zachowań w postaci odpowiednich schematów działania i instrukcji w zakresie przetwarzania danych osobowych, w celu zapewnienia należytej ich ochrony i zminimalizowania ryzyka jej naruszenia.

Stosowanie Polityki umożliwia zminimalizowanie czynników zagrażających działaniu jednostki oraz minimalizowanie skutków sytuacji kryzysowych zagrażających płynności funkcjonowania jednostki.

Poszczególne cele w zakresie bezpieczeństwa przetwarzania danych osobowych są realizowane poprzez stosowanie odpowiednich procedur i instrukcji oraz inne zabezpieczenia, które w szczególności obejmują:

- analizę i skategoryzowanie przetwarzanych w ramach podmiotu danych osobowych w ramach Rejestru czynności przetwarzania (załącznik nr 11),
- wdrożenie i zobowiązanie pracowników do stosowania Polityki ochrony danych osobowych,
- wprowadzenie procedury pisemnego upoważniania pracowników do przetwarzania danych osobowych w zakresie koniecznym do wykonywanych zadań – w odniesieniu do czynności przetwarzania wskazanych w przyjętym Rejestrze czynności przetwarzania,
- edukację pracowników w zakresie ochrony danych osobowych (załącznik nr 5),
- uświadomienie pracownikom konsekwencji, w tym dyscyplinarnych i karnych w przypadku naruszenia ochrony danych osobowych,
- wdrożenie zabezpieczeń organizacyjnych i technicznych w zakresie ochrony danych osobowych oraz monitorowanie ich skuteczności,
- coroczny przegląd i aktualizację dokumentacji związanej z Polityką, a także kategorii przetwarzanych danych osobowych i podstaw prawnych,
- coroczną analizę posiadanych zasobów pod kątem konieczności usunięcia zgromadzonych danych osobowych, co do których minął okres niezbędności przechowywania,
- monitorowanie i zgłaszanie incydentów związanych z bezpieczeństwem informacji, a także ich analiza i wdrażanie środków zaradczych i minimalizujących ryzyko pojawienia się podobnych zdarzeń w przyszłości,
- zapewnienie niszczenia nośników danych w sposób zapewniający ochronę osób, których dane dotyczą.

Celem działań związanych z ochroną danych osobowych jest zachowanie następujących zasad – dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość);
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);
- prawidłowe i w razie potrzeby uaktualniane (prawidłowość);
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane (ograniczenie przechowywania);

– przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych (w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem lub przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (integralność i poufność).

1.3 ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES STOSOWANIA

1. Polityka stanowi zbiór zasad i procedur przetwarzania danych osobowych i danych istotnych oraz zabezpieczenia ich przed nieuprawnionym dostępem.
2. Polityka składa się z następujących elementów:
   a) zadań i obowiązków ciążących na Administratorze Danych Osobowych oraz Inspektorze Danych Osobowych,
   b) wykazu zbiorów danych osobowych,
   c) określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
   d) wzorów dokumentów stosowanych przez Administratora Danych Osobowych.

1.4 DEFINICJE I WYJAŚNIENIE TERMINÓW

Sformułowania użyte w niniejszym dokumencie należy rozumieć w sposób następujący:

Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), zwana dalej „Ustawą".

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 (DZ.U. UE L 119/1).

Administrator danych osobowych (Administrator, ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – na potrzeby niniejszego dokumentu wskazuje się, że Administratorem danych jest Muzeum Miejskie w Żorach.

Administrator systemów informatycznych (ASI) – użytkownik uprzywilejowany, posiadający rozszerzone uprawnienia, umożliwiające zarządzanie systemami informatycznymi oraz innymi użytkownikami.

Anonimizacja – zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Dane wrażliwe – dane szczególnie chronione przez przepisy prawa. Zgodnie z RODO są to:

a) dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych,
b) dane genetyczne,
c) dane biometryczne,
d) dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
e) dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Przetwarzanie danych osobowych – to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych obejmująca zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

Pseudonimizacja – oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Inspektor Ochrony Danych Osobowych (IOD) – to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i tej polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Instrukcja zarządzania systemami informatycznymi – zespół norm oraz zasad obowiązujących w systemach informatycznych Administratora Danych Osobowych, służące m.in. zapewnieniu bezpieczeństwa oraz poufności danych.

Kwalifikacja archiwalna – ustalenie okresów przechowywania dokumentów, zbiorów dokumentów i akt spraw w oparciu o wymogi przepisów prawa, przydatność użytkową i naukową.

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Odbiorca oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyjątkiem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem krajowym; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

Ograniczenie przetwarzania polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

Profilowanie – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Strona trzecia oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane.

System Informatyczny (SI) – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur, przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie powoli na ustalenie tożsamości osoby, której dane dotyczą.

Zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zbiór danych oznacza każdy uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1 INFORMACJE OGÓLNE

1. Osobami odpowiedzialnymi za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, RODO, Polityki ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi są:
   a) Administrator danych osobowych (dalej zwany: Administrator, ADO),
   b) Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora.

2. Osoby wymienione w ust. 1 pkt b uzyskują stosowne upoważnienie do przetwarzania danych osobowych.
3. Wzór upoważnienia, o którym mowa powyżej stanowi załącznik nr 3 do Polityki.

2.2 ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem danych osobowych jest Muzeum Miejskie w Żorach, 44-240 Żory; ul. Muzealna 1/2, REGON: 277480212.

2.3 INSPEKTOR OCHRONY DANYCH OSOBOWYCH

1. Administrator powołuje Inspektora ochrony danych (załącznik nr 1).
2. Do zadań Inspektora Ochrony Danych Osobowych należy:
    a) stały nadzór nad treścią Polityki ochrony danych osobowych i Instrukcji zarządzania systemami informatycznymi,
    b) aktualizacja i modyfikacja ww. dokumentów,
    c) informowanie Administratora, podmiotów przetwarzających oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach związanych z przetwarzaniem danych osobowych spoczywających na nich na mocy przepisów prawa,
    d) monitorowanie przestrzegania przepisów ochrony danych osobowych poprzez dokonywanie czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (audyty) oraz opracowywanie sprawozdań (raporty z audytów),
    e) podejmowanie działań zwiększających świadomość ochrony danych osobowych personelu zatrudnionego u Administratora uczestniczącego w operacjach przetwarzania (szkolenia),
    f) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych,
    g) prowadzenie rejestru czynności przetwarzania, jeżeli taki obowiązek zaistnieje na podstawie przepisów prawa lub Inspektor uzna to za słuszne,
    h) prowadzenie ewidencji zbiorów danych osobowych,
    i) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem – zgodnie z art. 39. RODO,
    j) udział w kontrolach prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych.

2.4 ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Administrator danych osobowych może powołać (załącznik nr 2) Administratora systemów informatycznych (ASI).
2. Do zadań Administratora systemów informatycznych należy:
   a) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
   b) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   c) zapewnienie ciągłości działania systemów informatycznych,
   d) sprawne realizowanie procedur tworzenia kopii zapasowych,
   e) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

3. KONTROLA DOSTĘPU DO DANYCH OSOBOWYCH

Każdy pracownik przed rozpoczęciem przetwarzania danych osobowych:

- zapoznaje się z dokumentacją ochrony danych osobowych obowiązującymi w jednostce Administratora,
- otrzymuje pisemne upoważnienie Administratora z wyszczególnieniem czynności przetwarzania, co do których istnieje konieczność dostępu ze względu na obowiązki służbowe (zasada adekwatności).

3.1 OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, RODO oraz Polityki ochrony danych osobowych.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
3. Każda upoważniona osoba składa pisemne zobowiązanie o zachowaniu poufności zgodnie ze wzorem stanowiącym załącznik nr 4 do niniejszej Polityki.

3.2 UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważnienie do przetwarzania danych osobowych wydaje Administrator.
2. Cofnięcie upoważnienia następuje wraz z ustaniem stosunku prawnego pomiędzy pracownikiem lub współpracownikiem a Administratorem lub zmiany zakresu zadań.
4. Upoważnienie wydawane jest w formie pisemnej, zgodnie ze wzorem stanowiącym załącznik nr 3 do niniejszej Polityki.
5. Rejestr osób upoważnionych do przetwarzania danych opisanych w pkt. 1 prowadzi Inspektor w formie papierowej lub elektronicznej. Prowadzenie takiego rejestru jest obligatoryjne.

4. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Osoby odpowiedzialne za współpracę z firmami świadczącymi usługi/dostawy na rzecz Administratora, przed podpisaniem umowy zobowiązane są do analizy ewentualnej konieczności powierzenia danych osobowych.
2. Jeśli istnieje konieczność przekazania danych osobowych podmiotowi, z którym zawierana jest umowa, osoba odpowiedzialna za zawarcie umowy z ramienia Administratora, upewnia się, że realizator usługi/dostaw jest w stanie technicznie i organizacyjnie zapewnić bezpieczeństwo powierzonych danych osobowych.
3. W przypadku, gdy Administrator powierza przetwarzanie danych osobowych zewnętrznym podmiotom może się to odbyć wyłącznie w drodze umowy powierzenia zawartej w formie pisemnej.
4. Umowa powierzenia przetwarzania jest przygotowana lub zatwierdzona przez Inspektora Ochrony Danych. Wzór umowy stanowi załącznik nr 6 do Polityki.
5. Inspektor prowadzi wykaz podmiotów, którym powierzono przetwarzanie danych osobowych (załącznik nr 7).
6. W umowie powierzenia między innymi należy określić: zbiór, który zostanie przekazany, cel tego przekazania oraz zakres planowanego przetwarzania danych przez inny podmiot, obowiązki przetwarzającego, prawo do kontroli dokonywanej przez przekazującego, zakres odpowiedzialności przetwarzającego oraz czas obowiązywania umowy.
7. Pracownicy Administratora odpowiedzialni za realizację danej umowy są zobowiązani do monitorowania wypełnienia podjętych zobowiązań w zakresie ochrony danych osobowych oraz

do niezwłocznego informowania Administratora lub IOD w przypadku, gdy podejmą uzasadnione podejrzenie niedostatecznego ich wypełniania. W takim przypadku podejmowane są niezbędne środki w celu wyegzekwowania właściwego przestrzegania zapisów umowy, a gdy nie jest to możliwe, zaprzestaje się powierzania danych osobowych.

5. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. W trakcie przetwarzania danych osobowych w Muzeum Miejskim w Żorach stosowane są następujące zasady:
    a. zasada przejrzystości, zgodnie z którą wszelkie komunikaty związane z przetwarzaniem danych osobowych są prezentowane w łatwo dostępny, zrozumiały sposób, a także jasnym i prostym językiem,
    b. zasada zgodności z prawem, która wymaga, aby przetwarzanie danych osobowych było wykonywane na podstawie przesłanek legalności, tj. najczęściej zgody osoby fizycznej lub prawnie uzasadnionego interesu Administratora,
    c. zasada ograniczenia celu przetwarzania danych osobowych, która wymaga, aby dane były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
    d. zasada minimalizacji danych, która wymaga, aby dane osobowe były adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum,
    e. zasada prawidłowości danych, zgodnie z którą dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane,
    f. zasada ograniczenia przechowywania danych, która wymaga, aby okres przetwarzania danych był ograniczony do czasu, jaki jest niezbędny do tego, aby osiągnąć założony cel przetwarzania danych,
    g. zasada integralności i poufności, zgodnie z którą dane osobowe są przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich.
    h. rozliczalność – administrator danych jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie.
2. Podstawową przesłanką legalności jest dobrowolna zgoda na przetwarzanie danych osobowych.

3. W przypadku przetwarzania danych osobowych osoby niepełnoletniej wymagane jest otrzymanie zgody od jej prawnego opiekuna.
4. Administrator nie przetwarza w swoich działaniach danych wrażliwych. Do danych wrażliwych zaliczamy m.in. informację o zdolności do pracy pracownika (zaświadczenie lekarskie, L4), dokumenty dotyczące egzekucji komorniczych lub administracyjnych, orzeczenia dotyczące wyroków skazujących (art. 6 ust. 4 pkt c, art. 10).
5. Osoba, której dane są przetwarzane, ma prawo do: uzyskania informacji, dostępu do danych osobowych, sprostowania danych osobowych, usunięcia danych osobowych, ograniczenia przetwarzania danych osobowych, przenoszenia danych osobowych, sprzeciwu wobec przetwarzania danych osobowych, wniesienia skargi do organu nadzorczego, do bycia zapomnianą.

6. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych odpowiedzialni są wszyscy pracownicy.
2. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
3. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka" (załącznik nr 8). Zasada ta oznacza niepozostawianie materiałów zawierających dane osobowe i dane istotne w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
4. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
5. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
   Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem osób nieuprawnionych.

7. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po zakończeniu pracy, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem. Szczegółowe zasady postępowania w zakresie polityki kluczy opisane są w Instrukcji gospodarki kluczami.

7. MECHANIZM REAGOWANIA NA INCYDENTY. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik zobowiązany jest do reakcji na każde podejrzenie naruszenia ochrony danych osobowych. W przypadku zaistnienia incydentu – pracownik zabezpiecza, na ile to możliwe, dane osobowe oraz niezwłocznie informuje Administratora lub IOD.
2. W przypadku zauważenia naruszeń w dziedzinie IT, należy niezwłocznie poinformować o tym osobę odpowiedzialną za obszar IT. W każdym przypadku należy podjąć najszybszą drogę komunikacji. Osoby poinformowane, przełożeni, osoba odpowiedzialną za obszar IT w porozumieniu z Administratorem są zobowiązani do reakcji na każde zgłoszenie dotyczące incydentu naruszenia ochrony danych osobowych. Dokonują zabezpieczenia danych osobowych w możliwie najszybszy sposób, a następnie – w formie pisemnej (notatka służbowa, mail do ADO) opisują zaistniałą sytuację.
3. Osoby wskazane przez Administratora dokonują analizy, czy podejrzenie naruszenia ochrony danych osobowych miało znamiona incydentu oraz kwalifikują je do wymagających bądź niewymagających zgłoszenia do organu nadzorczego.
4. W przypadku stwierdzenia, że dany przypadek stanowi incydent naruszenia ochrony danych podlegający zgłoszeniu, Administrator lub osoba upoważniona dokonuje zgłoszenia zgodnie z wymogami prawnymi (maksymalnie do 72 godzin). Zgłoszenie zawiera:
   - opis charakteru naruszenia, w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorii i przybliżonej liczby wpisów danych, których dotyczy naruszenie;
   - imię, nazwisko i dane kontaktowe;
   - opis możliwych konsekwencji naruszenia oraz opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu i minimalizacji jego negatywnych skutków.

5. Dodatkowo osoby, których dane dotyczą, w sytuacji stwierdzenia, iż incydent może powodować naruszenie ich praw lub wolności, zostają o tym fakcie powiadomione. Termin powiadomienia uzależniony jest od stopnia naruszenia oraz zakresu danych, których dotyczy zdarzenie.
6. Każde zgłoszenie dotyczące naruszenia ochrony danych osobowych (nawet jeśli ostatecznie nie zostało zakwalifikowane jako incydent) zostaje odnotowane w Raporcie z naruszenia ochrony danych wraz z datą, opisem sytuacji i sposobu reakcji (załącznik nr 9). Każdy incydent podlega analizie pod kątem skuteczności zastosowanych środków, które miałyby zmniejszyć ryzyko pojawienia się podobnego zdarzenia w przyszłości.

8. KONTROLA LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Raz w roku – Administrator lub wskazana przez niego osoba w porozumieniu z pozostałymi pracownikami jest zobowiązany do zweryfikowania:
   - czy zakres przetwarzanych danych osobowych odpowiada zakresowi wskazanemu w Rejestrze czynności przetwarzania (adekwatność),
   - czy podstawa prawna wskazana w Rejestrze czynności przetwarzania jest nadal aktualna (legalność),
   - czy zakres przetwarzanych danych osobowych jest adekwatny do wykonywanych zadań (minimalizacja),
   - dokumentacji papierowej oraz plików elektronicznych w zakresie usunięcia danych osobowych, co do których minął okres przechowywania; okres niezbędny do realizacji celów przetwarzania danych osobowych (ograniczenie czasowe).
2. Po dokonaniu weryfikacji, o której mowa w punkcie powyżej ADO lub wskazana przez niego osoba dokonuje weryfikacji Rejestru czynności przetwarzania.

9. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodo-

bieństwie wystąpienia i wadze zagrożenia wdrożono odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

1. Co najmniej raz w roku, a w przypadku dużych zmian organizacyjnych czy planowania rozpoczęcia przetwarzania nowych rodzajów operacji, w których może wystąpić wysokie ryzyko naruszenia praw i wolności osób fizycznych przed przystąpieniem do przetwarzania – Administrator (lub wskazana przez niego osoba) weryfikuje, czy nie zachodzi konieczność dokonania oceny skutków dla ochrony danych osobowych (DPIA).
2. W przypadku wystąpienia nowych zagrożeń lub zwiększenia podatności na dane zagrożenia konieczne jest podjęcie odpowiednich kroków, aby stwierdzone ryzyka nie przekraczały poziomu średniego (wdrożenie dodatkowych zabezpieczeń) lub podjęcie decyzji ich akceptacji na poziomie wysokim.

10. ŚRODKI ORGANIZACYJNE, TECHNICZNE I FIZYCZNE WDROŻONE DO OCHRONY DANYCH OSOBOWYCH

10.1 ŚRODKI ORGANIZACYJNE ZASTOSOWANE DO OCHRONY DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych osobowych.
2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3. Opracowano i wdrożono Politykę ochrony danych osobowych.
4. Opracowano i wdrożono Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych (załącznik nr 10).
5. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
6. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
7. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy (w ramach upoważnienia do przetwarzania danych osobowych).
8. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym. Stosowane są chronione hasłem wygaszacze ekranu, blokowanie komputera przy opuszczeniu stanowiska pracy, polityka czystej drukarki, kosza i inne formy zabezpieczenia jak instrukcje, regulaminy, spisane zasady itp.

9. Przetwarzanie danych osobowych ograniczone jest do terenu Muzeum Miejskiego w Żorach.
10. W Muzeum Miejskim w Żorach stosuje się zasadę tzw. „czystego biurka".

10.2 ŚRODKI TECHNICZNE I FIZYCZNE ZASTOSOWANE DO OCHRONY DANYCH OSOBOWYCH

1. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęte są systemem kontroli dostępu (instrukcja gospodarki kluczami).
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych – monitorowanie korytarzy, klatki schodowej, wejść.
3. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej lub niemetalowej szafie (w zależności od zakresu danych osobowych w niej przechowywanych) w zamykanym pomieszczeniu niedostępnym dla osób postronnych (dane pracownicze itd.) lub w pomieszczeniu pod stałym osobowym nadzorem.
4. Serwerownia, archiwum, pomieszczenia, w których przechowywane są dokumenty kadrowe zabezpieczone za pomocą systemu przeciwpożarowego.
5. Serwerownia wyposażona jest w klimatyzację, bieżący pomiar temperatury i wilgotności.
6. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów dostosowanych do niszczenia dokumentacji lub zlecane specjalistycznej firmie.
7. Środki ochrony systemów informatycznych opisane są w Instrukcji zarządzania systemami informatycznymi.

ZAŁĄCZNIK NR 1

USTANOWIENIE INSPEKTORA OCHRONY DANYCH

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Ochrony Danych Osobowych oraz jako Administrator Danych Osobowych Muzeum Miejskiego w Żorach

wyznaczam

Panią/Pana ..... do pełnienia funkcji **Inspektora Ochrony Danych (IOD)** Muzeum Miejskiego w Żorach.

Zakres obowiązków oraz warunki pełnienia funkcji Inspektora Ochrony Danych określone są w art. 39 Rozporządzenia Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r. oraz w ustawie o ochronie danych osobowych z dnia 10 maja 2018 r.

.....	.....
Data i podpis osoby wyznaczonej do pełnienia funkcji IOD	Data i podpis Administratora Danych Osobowych

ZAŁĄCZNIK NR 2

USTANOWIENIE ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz jako Administrator Danych Osobowych Muzeum Miejskiego w Żorach

wyznaczam

Panią/Pana ..... na stanowisko **Administratora Systemów Informatycznych (ASI)** w Muzeum Miejskim w Żorach.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są Ustawą o ochronie danych osobowych z dnia 10 maja 2018 roku oraz dokumentacją z zakresu ochrony danych osobowych – Polityką Bezpieczeństwa wdrożoną dnia ...../ ..... / ..... (dd/mm/rrrr) w Muzeum Miejskim w Żorach.

.....	.....
Data i podpis osoby wyznaczonej do pełnienia funkcji ASI	Data i podpis Administratora Danych Osobowych

ZAŁĄCZNIK NR 3

WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

....., dn. .....

UPOWAŻNIENIE
do przetwarzania danych osobowych w Muzeum Miejskim w Żorach

Upoważniam Panią/Pana .....
Stanowisko .....
Dział .....

do przetwarzania danych osobowych w związku z wykonywaniem obowiązków wynikających z umowy *o pracę/umowy zlecenia/umowy o dzieło/umowy dotyczącej*.....
Upoważnienie obejmuje przetwarzanie następujących kategorii danych osobowych:
a) .....
b) .....
c) .....
d) .....
e) oraz na polecenie Administratora również inne dane, których przetwarzanie jest niezbędne do prawidłowej realizacji obowiązków pracowniczych zawartych w umowie.

Upoważnienie uprawnia Panią/Pana do przetwarzania danych osobowych w formie papierowej i elektronicznej. Zakres czynności wynika z treści zawartej z Panią/Panem umowy.
Jest Pani/Pan zobowiązana/y do ochrony danych osobowych przetwarzanych na polecenie Administratora, do zachowania ich w tajemnicy, przetwarzania zgodnie z prawem oraz wewnętrznymi regulacjami Administratora, jak również do zachowania w poufności stosowanych przez Muzeum Miejskie w Żorach środków bezpieczeństwa.

Data nadania upoważnienia .....

Upoważnienie wygasa z chwilą ustania Pana/Pani zatrudnienia w Muzeum Miejskim w Żorach lub z chwilą jego odwołania.

....

podpis Administratora podpis osoby upoważnionej

Upoważnienie zostaje wydane na podstawie: art. 29 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 (RODO).

OŚWIADCZENIE

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Muzeum Miejskim w Żorach (w szczególności z dokumentacją Polityki ochrony danych osobowych). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie 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 odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

ZAŁĄCZNIK NR 4

WZÓR OŚWIADCZENIA O ZOBOWIĄZANIU SIĘ DO ZACHOWANIA POUFNOŚCI

....., dn. .....

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y .....
zamieszkała/y w .....
zatrudniona/y w .....
na stanowisku .....

zobowiązuję się zachować w tajemnicy wszelkie informacje, do których uzyskałem/łam dostęp w związku z zatrudnieniem w Muzeum Miejskim w Żorach, w tym informacje zawarte w systemach informatycznych.

Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

.....
podpis

ZAŁĄCZNIK NR 5

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W MUZEUM MIEJSKIM W ŻORACH

Nr	Imię i nazwisko	Stano-wisko/ dział	Data nadania upoważnienia	Data odwołania upoważnienia	Czynności przetwa-rzania (poz. z RCP)	Systemy informa-tyczne, do których nadano dostęp	Dostęp do pomieszczeń szczególnie chronionych (serwerownia, kadry, archiwum)

ZAŁĄCZNIK NR 6

WZÓR UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych
zawarta dnia _____ pomiędzy:
(zwana dalej „Umową")

_____ (*dane podmiotu, który umowę zawiera)

zwany w dalszej części umowy „Podmiotem przetwarzającym"
reprezentowana przez:
_____

oraz

_____ (*dane podmiotu, który umowę zawiera)

zwany w dalszej części umowy „Administratorem danych" lub „Administratorem"
reprezentowana przez:
_____

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego Rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2
Zakres i cel przetwarzania danych

1. Zakres przetwarzania obejmuje ..... (wprowadzanie, wgląd, modyfikację, drukowanie, usuwanie, archiwizację, przesyłanie itp.) danych osobowych w zbiorach Powierzającego: .....
2. Z tytułu wykonywania świadczeń określonych w niniejszej Umowie Podmiotowi przetwarzającemu nie przysługuje dodatkowe wynagrodzenie ponad to, które zostało określone w Umowie głównej ..... (numer umowy z dnia .....).

§3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych osobowych do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa / zwraca Administratorowi wszelkie dane osobowe (należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32–36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin od zdarzenia.

§4
Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum ..... (*należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli) jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (*Administrator termin może określić dowolnie).
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §5 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6
Odpowiedzialność Podmiotu przetwarzającego

Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Urząd Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7
Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony*
   od ..... do .....
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem ..... * okresu wypowiedzenia.

§8
Rozwiązanie umowy

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z Umową;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§9
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych (*lub Podmiotu przetwarzającego w zależności od postanowień stron).

....
Administrator Danych Osobowych Podmiot przetwarzający

ZAŁĄCZNIK NR 7

WYKAZ PODMIOTÓW, KTÓRYM ADMINISTRATOR DANYCH OSOBOWYCH POWIERZYŁ PRZETWARZANIE DANYCH OSOBOWYCH

Wykaz podmiotów, którym powierzono przetwarzanie danych

Lp.	Nazwa podmiotu	Data zawarcia umowy powierzenia

ZAŁĄCZNIK NR 8

ZASADA CZYSTEGO BIURKA W MUZEUM MIEJSKIM W ŻORACH

1. Niniejsza Zasada czystego biurka (dalej: Zasada) obowiązuje wszystkich pracowników Muzeum Miejskiego w Żorach od dnia wdrożenia Polityki Ochrony Danych Osobowych na terenie całego zakładu pracy.
2. Na potrzeby niniejszej Zasady za pracowników Administratora uważa się pracowników w rozumieniu art. 2 ustawy z 26 czerwca 1974 r. – Kodeks Pracy, zatrudnionych u Administratora danych oraz wszystkie pozostałe osoby, które wykonują u Administratora pracę na innej podstawie niż stosunek pracy, a także osoby prowadzące jednoosobowe działalności gospodarcze współpracujące z Administratorem oraz osoby, które zostały przyjęte na praktyki, staż, wolontariat.
3. Pracownicy zobowiązani są do przechowywania na biurku tylko tych dokumentów, które są im niezbędne w danym momencie do wykonania bieżących zadań.
4. Jeśli pracownicy korzystają w biurze z tablic korkowych lub magnetycznych nie powinni umieszczać na nich informacji zawierających dane osobowe.
5. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy. Na osobę, której klucz powierzono, przechodzi pełna odpowiedzialność za realizację Zasady.
6. Obowiązki określone w pkt. 5 pracownik powinien wykonać również w przypadku opuszczenia stanowiska pracy na czas dłuższy niż 30 minut.
7. W sytuacjach nagłych, związanych w szczególności ze stanem zdrowia pracownika lub przedłużającą się nieobecnością w biurze, za realizację Zasady w jego imieniu odpowiadają solidarnie pracownicy, których stanowiska pracy znajdują się najbliżej.
8. Po zakończonej pracy pracownik powinien pozostawić na biurku jedynie przedmioty związane z wyposażeniem stanowiska pracy, takie jak np. materiały biurowe, telefon itp.
9. Pracownik zobowiązany jest na bieżąco niszczyć te dokumenty, które przestały mu być potrzebne. Dokumenty powinny być niszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji.

10. Pracownik jest zobowiązany do ustawienia wygaszacza ekranu na użytkowanym przez niego komputerze. Wygaszacz powinien włączać się automatycznie po okresie bezczynności użytkownika, trwającym nie dłużej niż 5 minut. W przypadku wznowienia aktywności, powrót do pracy z komputerem powinien być możliwy jedynie po podaniu odpowiedniego hasła.
11. W przypadku czasowego opuszczenia stanowiska pracy, pracownik jest zobowiązany do każdorazowego blokowania komputera poprzez włączenie wygaszacza ekranu.
12. Po zakończeniu pracy pracownik powinien wylogować się z systemu i wyłączyć komputer.
13. Obowiązuje zakaz trzymania na biurku wszelkich produktów spożywczych, których posiadanie grozi rozlaniem płynu.
14. Spożywanie posiłków możliwe jest wyłącznie w miejscu do tego wyznaczonym przez pracodawcę.

Oświadczam, iż zapoznałem się z niniejszą Zasadą czystego biurka i zobowiązuję się do jej stosowania.

Żory, dnia .....

.....

(podpis składającego oświadczenie)

ZAŁĄCZNIK NR 9

RAPORT Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Data ..... godzina .....

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

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

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
   .....

5. Podjęte działania:
   .....

6. Wstępna ocena przyczyn wystąpienia naruszenia:
   .....

7. Postępowanie wyjaśniające i naprawcze:
   .....

....

(podpis pracownika) (data i podpis Inspektora Ochrony Danych)

ZAŁĄCZNIK NR 10

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W MUZEUM MIEJSKIM W ŻORACH

1. Postanowienia ogólne
2. Metody i środki uwierzytelniania w systemach informatycznych
3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemów
4. Procedury tworzenia kopii zapasowych danych
5. Przechowywanie nośników zawierających dane oraz kopii zapasowych
6. Środki ochrony systemów informatycznych
7. Procedury wykonywania przeglądów i konserwacji systemów

1. Postanowienia ogólne

1.1. Instrukcja zarządzania systemami informatycznymi (dalej: Instrukcja) jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania systemem informatycznym Muzeum Miejskiego w Żorach. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, w szczególności zaś osoby pełniące funkcje:

- administratora systemów informatycznych – jeśli został wyznaczony,
- kierowników bądź osób sprawujących nadzór nad funkcjonowaniem poszczególnych komórek organizacyjnych,
- inne osoby wskazane przez Administratora Danych Osobowych, w tym osoby z podmiotów zewnętrznych współpracujące z Muzeum Miejskim w Żorach współuczestniczące w procesie przetwarzania danych osobowych.

1.2. Określenia i skróty użyte w Instrukcji:

- Administrator Danych Osobowych – dyrektor Muzeum Miejskiego, zwany dalej Administratorem;

- Administrator Systemów Informatycznych (Administrator SI) – użytkownik uprzywilejowany, posiadający rozszerzone uprawnienia, umożliwiające zarządzanie systemami informatycznymi oraz innymi użytkownikami;
- Użytkownik systemu – osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu;
- Hasło – ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
- Dane wrażliwe – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym.

2. Metody i środki uwierzytelniania w systemach informatycznych

2.1. Naczelną zasadą bezpieczeństwa systemów/aplikacji jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelnienia użytkowników systemów/aplikacji ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

2.1.1. W systemach/aplikacjach informatycznych Muzeum Miejskiego w Żorach stosuje się uwierzytelnianie jednostopniowe, na poziomie dostępu do systemu/aplikacji.

2.1.2. Do uwierzytelnienia użytkownika w systemie/aplikacji używa się identyfikatorów i haseł:

a) stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizację zasady rozliczalności w systemach Muzeum Miejskiego w Żorach,

b) zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi (nie dopuszcza się, aby użytkownik korzystał z kont: Administrator, gość, a także z konta innego użytkownika),

c) ograniczenie dostępu do informacji jedynie do kręgu użytkowników uprawnionych (autoryzowanych) wymaga przyjęcia odpowiednio dobranej polityki stosowania haseł.

2.1.3. W Muzeum Miejskim w Żorach stosuje się poziom bezpieczeństwa przetwarzania danych adekwatnie do klasyfikacji tych danych w systemach/aplikacjach. W związku z powyższym, obowiązujące są dwa poziomy bezpieczeństwa:

a) poziom podstawowy – dla systemów/aplikacji, w których nie są przetwarzane dane osobowe wrażliwe oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi się składać z co najmniej 6 znaków,

b) poziom podwyższony – dla systemów/aplikacji, w których są przetwarzane dane wrażliwe oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi się składać z co najmniej 8 znaków i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2.1.4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych bezpośrednio kojarzących się z użytkownikiem.

2.1.5. Hasło nie może być ujawnione innej osobie nawet po utracie ważności hasła.

2.1.6. Hasło musi być zmieniane przez użytkownika nie rzadziej niż raz w roku.

2.1. Procedura zarządzania środkami uwierzytelnienia:

a) użytkownik systemu ustala swoje, znane tylko jemu hasło,

b) użytkownik systemu w dowolnym momencie może zmienić swoje hasło dostępu do systemu/aplikacji,

c) użytkownik – Administrator zapisuje hasło do systemu i umieszcza je w kopercie, a następnie przekazuje zamkniętą kopertę do przechowania w wyznaczonej do tego celu szafie metalowej ulokowanej w archiwum merytorycznym. Koperta taka może być awaryjnie udostępniona innemu Administratorowi za zgodą Administratora Danych Osobowych,

d) obowiązuje bezwzględny zakaz notowania w jakiekolwiek formie, poza wskazaną powyżej, obecnych oraz wygasłych haseł dostępu.

3. Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

3.1. Procedura rozpoczęcia pracy:

a) uruchomić komputer wchodzący w skład systemu informatycznego i zalogować się podając własny identyfikator i hasło dostępu,

b) uruchomić wybrany system/aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane),
c) zalogować się do systemu/aplikacji w sposób analogiczny do przedstawionego powyżej.

3.2. Procedura zawieszenia pracy w systemie/aplikacji. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie komputera. Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem lub wylogowania się z systemu.

3.3. Procedura zakończenia pracy w systemie:
a) zamknąć system/aplikację,
b) zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
c) wyłączyć monitor i inne urządzenia peryferyjne,
d) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

3.4. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

4. Procedury tworzenia kopii zapasowych danych

4.1.1. Każde indywidualne stanowisko komputerowe, do którego dostęp posiadają pracownicy Muzeum Miejskiego w Żorach, traktowane jest jako serwer dla swojego klienta.

4.1.2. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane lokalnie na wyznaczonej do tego celu partycji dysku.

4.1.3. W celu zapewnienia optymalnego poziomu ochrony danych osobowych gromadzonych w systemach informatycznych Muzeum Miejskiego w Żorach (MONA – program do ewidencji zbiorów), przyjęto do stosowania zasadę przechowywania kopii danych na wyznaczonych do tego celu dyskach zewnętrznych.

4.2.1. Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na integralnych dyskach stanowiskowych wykonywane są w cyklu miesięcznym „ręcznie".

4.2.2. Zasady przechowywania kopii:
a) kopie zapasowe zbioru danych oraz oprogramowania i narzędzi programistycznych zastosowanych do przetwarzania danych są przechowywane w przeznaczonej do tego celu metalowej szafie, znajdującej się w archiwum merytorycznym,
b) dostęp do metalowej szafy ma tylko: Administrator Danych Osobowych.

5. Przechowywanie nośników informacji zawierających dane oraz kopii zapasowych

5.1. Elektroniczne nośniki informacji:

a) dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (np. nośnikach flaszowych, płytach CD/DVD, dyskach twardych) są własnością Muzeum Miejskiego w Żorach,

b) wyżej wymienione elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych,

c) po zakończeniu pracy przez użytkowników systemów/aplikacji, ww. elektroniczne nośniki informacji są przechowywane w meblach biurowych ze sprawnym zamknięciem lub w zamykanych pudełkach służących do ich przechowywania,

d) elektroniczne nośniki informacji, o których mowa powyżej, powinny być oznaczone w sposób umożliwiający ich identyfikację.

5.2. Przekazywanie i niszczenie elektronicznych nośników informacji:

a) elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez Administratora Danych Osobowych,

b) dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone przed odczytem (minimum hasłem),

c) dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych.

6. Środki ochrony systemów informatycznych

6.1. Poniżej przedstawiono zasady ochrony systemów przetwarzania danych przed tzw. „szkodliwym oprogramowaniem" oraz próbami penetracji przez osoby nieuprawnione.

6.2. Ochrona antywirusowa:

a) za ochronę antywirusową odpowiada osoba wyznaczona przez Administratora Danych Osobowych,

b) czynności związane z ochroną antywirusową systemu informatycznego wykonuje użytkownik systemu, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego,

c) oprogramowanie antywirusowe jest instalowane na wszystkich stanowiskach komputerowych podłączonych do sieci,
d) aktualizacja oprogramowania antywirusowego odbywa się codziennie, w sposób automatyczny,
e) użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.

7. Procedury wykonywania przeglądów i konserwacji systemu

7.1.1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system/aplikacja.
7.1.2. Przeglądy i konserwacja urządzeń:
a) przeglądy i konserwacje urządzeń wchodzących w skład platformy sprzętowej dla danego systemu/aplikacji powinny być wykonywane w terminach określonych przez producenta sprzętu,
b) nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
7.2.1. Przegląd systemów/aplikacji i narzędzi programistycznych przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
a) zmiany wersji oprogramowania systemu/aplikacji,
b) zmiany wersji oprogramowania na stanowisku komputerowym użytkownika,
c) zmiany systemu operacyjnego na stanowisku komputerowym użytkownika,
d) wykonania zmian w systemie/aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu.
7.2.2. Za prawidłowość przeprowadzenia procesu przeglądu i konserwacji systemu/aplikacji odpowiada osoba wyznaczona przez Administratora Danych Osobowych.
7.3. Konserwacja systemów/aplikacji wykorzystywanych przez użytkowników.
7.3.1. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu/aplikacji potrzeby wprowadzenia zmian pozwalających dostosować funkcjonalność systemu/aplikacji do obsługi bieżących i planowanych potrzeb Muzeum Miejskiego w Żorach. Zgłoszenia kierowane są osoby wyznaczonej przez Administratora Danych Osobowych.

ZAŁĄCZNIK NR 11

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA

Wykaz podmiotów, którym powierzono przetwarzanie danych

Rejestr czynności przetwarzania danych osobowych	
Nazwa administratora danych lub podmiotu przetwarzającego / przedstawiciela administratora lub podmiotu przetwarzającego	
Współadministratorzy	
Inspektor ochrony danych	
Cel przetwarzania	
Opis kategorii osób	
Kategorie odbiorców	
Kategorie danych osobowych	
Informacje o przekazaniu do państwa trzeciego lub organizacji międzynarodowej	
Planowany termin usunięcia danych osobowych	
Opis technicznych i organizacyjnych środków bezpieczeństwa	

ARCHIWIZACJA ZASOBÓW

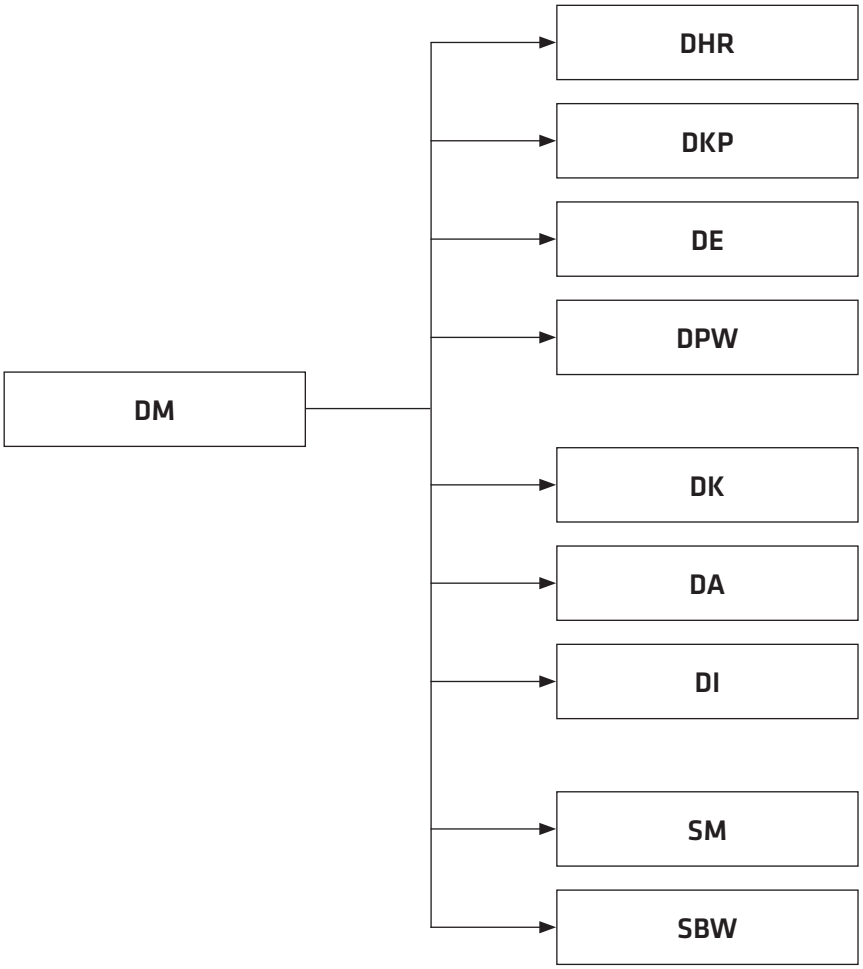
1. ARCHIWIZACJA ZASOBÓW DOKUMENTACJI PAPIEROWEJ / ARCHIWIZACJA DOKUMENTACJI ELEKTRONICZNEJ

Archiwizacja zasobów dokumentacyjnych gromadzonych w sposób tradycyjny odbywa się zgodnie z wytycznymi zawartymi w Instrukcji archiwum Muzeum Miejskiego w Żorach.

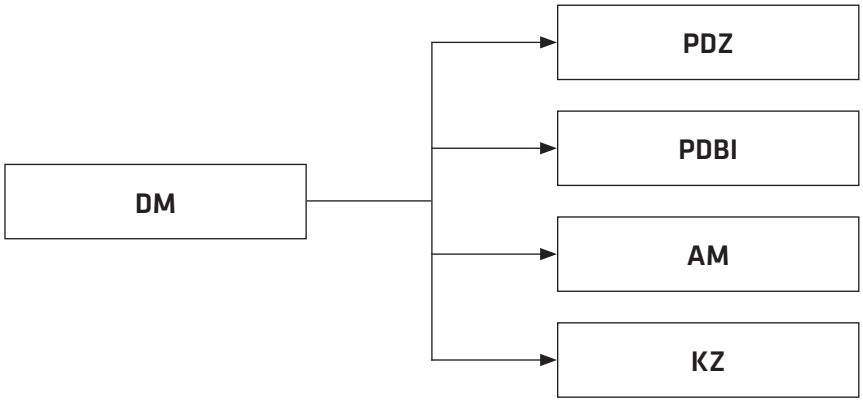
Archiwizacja zasobów elektronicznych odbywa się zgodnie z wytycznymi zawartymi w Instrukcji zarządzania systemami informatycznymi.

Archiwizacja dokumentacji gromadzonej w sposób tradycyjny oraz elektroniczny odbywa się zgodnie ze schematem.

Schemat organizacyjny Muzeum Miejskiego w Żorach (komórkowy)



Schemat organizacyjny Muzeum Miejskiego w Żorach (zadania delegowane)



Struktura archiwizacji została opracowana na podstawie dokumentów informujących o:

- zasobach sprzętowych na każdym stanowisku gromadzącym dane,
- zasobach archiwalnych gromadzonych na każdym stanowisku.

Formularz informacji o zasobach archiwalnych gromadzonych na stanowisku

Stanowisko	Nazwa zgodnie z JRWA		Opis gromadzonej dokumentacji	Kategoria akt	Dokumentacja elektroniczna	Dokumentacja papierowa	Osoba odpowiedzialna za zasoby

Formularz informacji o zasobach sprzętowych na każdym stanowisku

Stanowisko	Pomiesz-czenie	Nazwa komputera	Sprzęt	System/ licencja	Programy/ licencje	Data wygaśnięcia	Osoba odpowie-dzialna za zasoby

Struktura zapisu

A. Archiwizacja danych, po ich uprzednim uporządkowaniu odbywa się zgodnie z harmonogramem wewnętrznym wynikającym z Instrukcji zarządzania systemami informatycznymi.

B. Dane zapisywane są w systemie numerycznym – foldery oraz numeryczno-literowym – pliki.
Ścieżka dostępu nie może przekraczać 253 znaków.
W zapisie nie mogą być używane polskie znaki.

Struktura archiwizacji dokumentacji muzealnej opracowywane jest przez:

- Pełnomocnika ds. bezpieczeństwa informacji,
- Archiwistę Muzeum Miejskiego w Żorach.

Wskazane osoby odpowiadają również za aktualizacje struktury archiwizacji dokumentacji muzealnej, jeżeli wymagać będą tego zmiany w zakresie „Standardów kontroli zarządczej Muzeum Miejskiego w Żorach".

2. INSTRUKCJA O ORGANIZACJI I ZAKRESIE DZIAŁANIA ARCHIWUM MUZEUM MIEJSKIEGO W ŻORACH

I. POSTANOWIENIA OGÓLNE

1. Niniejsza instrukcja ustala organizację, zadania i zakres działania Archiwum Muzeum. Instrukcja reguluje tryb przejmowania dokumentacji z komórek organizacyjnych, ich przechowywanie i ewidencjonowanie w Archiwum Muzeum. Określa zasady udostępniania dokumentacji oraz sposób postępowania z materiałami archiwalnymi i dokumentacją niearchiwalną.

2. Użyte w niniejszej instrukcji określenia oznaczają:
   - archiwum Muzeum – komórka Muzeum powołaną do gromadzenia, przechowywania, zabezpieczania, ewidencjonowania i udostępniania dokumentacji, a także brakowania dokumentacji niearchiwalnej;
   - dokumentacja – zbiór wszelkiego rodzaju dokumentów, księgi, korespondencja, dokumentacja finansowa, statystyczna, mapy, plany i projekty – niezależnie od techniki ich wykonania (rękopisy, maszynopisy, druki) i inna dokumentacja utrwalona sposobem mechanicznym lub elektronicznym;
   - komórka organizacyjna Muzeum – komórka powołana do wykonywania określonych zadań, wymieniona w Regulaminie organizacyjnym Muzeum;
   - pracownik Archiwum Muzeum – osoba wskazana przez dyrektora pełniąca funkcję pracownika Archiwum Muzeum na podstawie delegacji uprawnieniowo-zadaniowej;
   - sprawa – zdarzenie lub stan rzeczy wymagające podjęcia i wykonania czynności urzędowych;
   - spis spraw – formularz służący do chronologicznego rejestrowania spraw wpływających lub zapoczątkowanych w Muzeum; prowadzi się go oddzielnie dla każdego hasła (teczki) w wykazie akt z zaznaczoną kwalifikacją archiwalną;
   - teczka spraw (aktowa) – skoroszyt, segregator, teczka wiązana (aktowa) itp., służąca do przechowywania jednorodnych lub rzeczowo pokrewnych akt spraw ostatecznie załatwionych, objętych tą samą grupą akt ustalonych wykazem akt;
   - wykaz akt – rzeczowa klasyfikacja akt powstających w toku działalności Muzeum, oznaczona w poszczególnych pozycjach symbolem, hasłem i kategorią archiwalną;
   - znak sprawy – zespół symboli określających przynależność sprawy do określonej jednostki organizacyjnej i do określonej grupy spraw;
   - znak akt – zespół symboli określających przynależność sprawy do określonej komórki organizacyjnej i do określonej grupy rzeczowego wykazu akt.

3. Rozróżnia się następujące kategorie archiwalne:
   a) dla oznaczenia kategorii dokumentacji niearchiwalnej, tj. mającej czasowe znaczenie praktyczne stosuje się symbol „B" z dodaniem cyfr arabskich, oznaczających okres przechowywania, po upływie którego dokumentacja ta podlega brakowaniu, czyli ocenie przydatności dla celów praktycznych i przekazaniu na makulaturę. Okres przechowywania liczy się w pełnych latach kalendarzowych, tj. poczynając od 1 stycznia roku następnego po załatwieniu sprawy,
   b) dla oznaczenia kategorii dokumentacji, którą po upływie danego okresu przechowywania poddaje się ekspertyzie Archiwum Państwowego, stosuje się symbol „BE",
   c) dla oznaczenia kategorii dokumentacji posiadającej krótkotrwale znaczenie praktyczne, którą po pełnym wykorzystaniu przeznacza się bezpośrednio na makulaturę, stosuje się symbol „Bc".

4. Dokumentacja niearchiwalna podlega brakowaniu po upływie okresu przechowywania. Okres ten jest podany w „Jednolitym rzeczowym wykazie akt Muzeum Miejskiego w Żorach" (dalej: JRWA) stanowiącym załącznik Instrukcji kancelaryjnej. JRWA powinny posiadać wszystkie komórki organizacyjne.

II. ORGANIZACJA ARCHIWUM MUZEUM, JEGO ZADANIA I ZAKRES DZIAŁANIA

1. Archiwum Muzeum jest komórką, nadzorującą postępowanie z dokumentacją w Muzeum.

2. Archiwum Muzeum zajmuje się przejmowaniem dokumentacji niepotrzebnej do bieżącego urzędowania komórki organizacyjnej, jej przechowywaniem, ewidencjonowaniem, udostępnianiem, brakowaniem oraz zabezpieczaniem powierzonego narodowego zasobu.

3. Pracownik Archiwum jest odpowiedzialny za jego prawidłowe funkcjonowanie, za zabezpieczenie archiwum i jego dokumentacji przed zniszczeniem. Do obowiązków pracownika archiwum należy:
   a) znajomość Instrukcji kancelaryjnej, JRWA, Instrukcji o organizacji i zakresie działania Archiwum Muzeum, oraz Regulaminu organizacyjnego Muzeum obowiązujących w przeszłości i obecnie,

b) przejmowanie dokumentacji z komórek organizacyjnych Muzeum,
c) prowadzenie ewidencji przejętej do archiwum dokumentacji,
d) przechowywanie i zabezpieczanie dokumentacji,
e) udostępnianie dokumentacji,
f) nadzór nad postępowaniem z dokumentacją w poszczególnych komórkach organizacyjnych Muzeum,
g) brakowanie dokumentacji niearchiwalnej (kat. B),
h) sporządzanie rocznego planu pracy i sprawozdania,
i) protokolarne przekazanie Archiwum Muzeum w przypadku zmiany na stanowisku pracownika archiwum.

4. Pomieszczenie Archiwum Muzeum powinien spełniać następujące warunki:
a) mieścić się w budynku biurowym,
b) składać się z części biurowej i magazynu,
c) być suchym, równomiernie ogrzewanym w ciągu roku, wolnym od przewodów kanalizacyjnych, widnym i powinno mieć możliwość wietrzenia; optymalne warunki przechowywania: temperatura powietrza w granicach 14°C–18°C, wilgotność 55–65% wilgotności względnej,
d) powinno być zabezpieczone przed włamaniem,
e) archiwum winno mieć regały metalowe stojące minimum 10 cm od ściany, z przejściem między nimi 70–90 cm, o szerokości półek około 40 cm,
f) powinno być wyposażone w sprzęt przeciwpożarowy (gaśnicę proszkową, koce gaśnicze z włókna szklanego i worki ewakuacyjne) oraz higrometr i termometr oraz w drabinki umożliwiające dostęp do wysokich półek i lniane zasłony, rolety lub żaluzje w oknach, chroniące akta przed promieniowaniem słonecznym.

5. Zabrania się w archiwum:
a) instalowania pieców żelaznych i otwartych grzejników,
b) palenia tytoniu,
c) tarasowania przejść między regałami,
d) składowania w archiwum rzeczy i przedmiotów niebędących mieniem archiwum.

6. Prawo wstępu do Archiwum Muzeum mają tylko w obecności pracownika archiwum, jego przełożeni, przedstawiciele archiwów państwowych, innych organów kontrolnych po okazaniu upoważnienia oraz pracownicy korzystający z dokumentacji zgromadzonej w archiwum.

III. PRZEJMOWANIE DOKUMENTACJI Z KOMÓREK ORGANIZACYJNYCH MUZEUM PRZEZ ARCHIWUM MUZEUM

1. Dokumentację spraw ostatecznie załatwionych przechowuje się w komórkach organizacyjnych Muzeum przez okres 2 lat, licząc od zakończenia roku kalendarzowego, w którym sprawa została załatwiona. Po upływie tego terminu Archiwum Muzeum przejmuje dokumentację z komórek organizacyjnych Muzeum.

2. Dokumentację przed przekazaniem do Archiwum Muzeum porządkuje komórka organizacyjna, która ją wytworzyła.

3. Przez uporządkowanie rozumie się ułożenie akt w poszczególnych teczkach w kolejności spisu spraw, a w obrębie sprawy – chronologicznie od najwcześniejszego pisma na wierzchu teczki do ostatniego na spodzie oraz opisanie teczki.

4. Opis teczki winien zawierać na stronie tytułowej:
   a) na środku u góry: Muzeum Miejskie w Żorach i nazwa komórki organizacyjnej, w której akta powstały,
   b) w lewym górnym rogu: znak akt złożony z symbolu komórki organizacyjnej i symbolu hasła wg JRWA,
   c) w prawym górnym rogu: kategorię archiwalną akt wg JRWA oraz okres ich przechowywania,
   d) na środku: tytuł akt, tj. pełne hasło z wykazu akt uzupełnione określeniem rodzaju dokumentacji,
   e) bezpośrednio pod tytułem: daty skrajne, tj. daty założenia pierwszej i ostatniej sprawy.

5. Komórki organizacyjne Muzeum przekazują dokumentację w układzie zgodnym ze spisem zdawczo-odbiorczym akt. Spis zdawczo-odbiorczy sporządza się dla akt kat. B w trzech egzemplarzach. Jeden egzemplarz otrzymuje komórka organizacyjna przekazująca akta. Dwa egzemplarze spisów zdawczo-odbiorczych zostają w Archiwum Muzeum.

6. Pracownik Archiwum sprawdza zgodność spisu zdawczo-odbiorczego ze stanem faktycznym. Jeżeli dokumentacja jest nieuporządkowana lub niezgodna ze spisem zdawczo-odbiorczym, pracownik archiwum odmawia przejęcia akt do Archiwum Muzeum, a następnie informuje o przyczynach odmowy swojego przełożonego.

7. Spis zdawczo-odbiorczy podpisuje kierownik komórki organizacyjnej i pracownik prowadzący Archiwum Muzeum.

IV. EWIDENCJONOWANIE I PRZECHOWYWANIE DOKUMENTACJI W ARCHIWUM MUZEUM

1. Spisy zdawczo-odbiorcze rejestruje się w wykazie spisów zdawczo-odbiorczych (załącznik nr 2 do niniejszej Instrukcji) w kolejności wpływu i nadaje się im numery bieżące wykazu. Jeden egzemplarz spisów zdawczo-odbiorczych wszywa się do teczki w kolejności numerów spisów. Drugi egzemplarz spisów zdawczo-odbiorczych (kopię) przechowuje się w teczkach, oddzielnie dla każdej komórki organizacyjnej.

2. Pracownik Archiwum oznacza przejętą dokumentację sygnaturą Archiwum Muzeum. Składa się na nią numer spisu zdawczo-odbiorczego wg wykazu spisów zdawczo-odbiorczych, łamany przez kolejną pozycję spisu, pod którą teczka figuruje w tym spisie.

3. Dokumentacja przechowywana w Archiwum musi być objęta ewidencją prowadzoną na bieżąco. Ewidencja ta umożliwia kontrolę liczby i stanu przechowywania akt.

4. Ewidencję zasobu archiwum stanowią:
   a) spisy zdawczo-odbiorcze – załącznik nr 1 do niniejszej Instrukcji,
   b) wykazy spisów zdawczo-odbiorczych, do których wpisuje się poszczególne spisy zdawczo-odbiorcze w kolejności ich wpływu i nadaje się im kolejną numerację – załącznik nr 2 do niniejszej Instrukcji,
   c) karty udostępniania akt – załącznik nr 3 do niniejszej instrukcji,
   d) spisy dokumentacji niearchiwalnej (aktowej i technicznej) przeznaczonej na makulaturę lub zniszczenie – załącznik nr 4 i 5 do niniejszej Instrukcji,
   e) protokoły oceny dokumentacji niearchiwalnej – załącznik nr 6 do niniejszej Instrukcji.

   Środki ewidencyjne wymienione w punkcie 4 powinny być przechowywane w oddzielnych teczkach. Natomiast karty udostępniania akt – punkt 4, podpunkt c przechowuje się przez okres dwóch lat licząc od daty zwrotu akt.

5. Dokumentację w Archiwum Muzeum przechowuje się komórkami organizacyjnymi z pozostawieniem miejsca na nowe nabytki. Regały odpowiednio oznacza się symbolami komórek organizacyjnych.

6. Na półkach dokumentację układa się pionowo, od lewej do prawej strony (systemem bibliotecznym) lub jedna na drugiej teczce w kolejności sygnatur, czyli od dołu ku górze.

7. Przechowywaną dokumentację, pracownik Archiwum poddaje konserwacji profilaktycznej (odpowiednie warunki przechowywania) i naprawia skutki ewentualnych zniszczeń zgodnie z posiadaną wiedzą i możliwościami technicznymi.

8. Prawidłowa ewidencja i przechowywanie dokumentacji w Archiwum Muzeum mają na celu sprawne jej udostępnianie, zabezpieczanie oraz brakowanie dokumentacji niearchiwalnej (tj. akt kat. B).

V. UDOSTĘPNIANIE DOKUMENTACJI ZGROMADZONEJ W ARCHIWUM MUZEUM

1. Udostępnianie dokumentacji może się odbywać na miejscu w Archiwum Muzeum lub poza lokalem archiwum poprzez wypożyczanie.

2. Dokumentacja ta może być wykorzystywana w celach służbowych lub naukowo-badawczych.

3. Udostępnianie odbywa się na podstawie karty udostępniania (załącznik nr 3 do niniejszej Instrukcji) i tylko na czas określony. Wyszukiwaniem, udostępnianiem lub wypożyczaniem zajmuje się wyłącznie pracownik Archiwum. W miejsce wypożyczonych akt wkłada się zakładkę z sygnaturą wypożyczonych akt.

4. Wypożyczanie poza teren Muzeum odbywa się tylko za zgodą dyrektora Muzeum.

5. Udostępnianie dokumentacji do celów naukowo-badawczych, odbywa się wyłącznie w pomieszczeniu Archiwum Muzeum i wymaga pisemnej zgody dyrektora Muzeum.

6. Korzystający z dokumentacji przyjmuje na siebie odpowiedzialność za materiały, z których korzysta oraz za terminowy ich zwrot do Archiwum Muzeum.

7. Zabrania się w szczególności:
   a) wyjmowania pism i dokumentów z udostępnionych lub wypożyczonych teczek,
   b) nanoszenia na tych dokumentach jakichkolwiek zapisów lub znaków,
   c) niszczenia dokumentów.

8. Wypożyczając dokumentację pracownik archiwum sprawdza stan jej zachowania. Tak samo postępuje przy jej zwrocie do Archiwum Muzeum.

9. W razie stwierdzenia braków lub uszkodzeń pracownik Archiwum sporządza protokół w trzech egzemplarzach, podpisywany przez zwracającego akta, jego przełożonego i pracownika Archiwum. Jeden egzemplarz załącza się w miejsce zaginięcia akt, drugi dostaje kierownik komórki organizacyjnej, której akta zaginęły, a trzeci przechowuje się w oddzielnej teczce w Archiwum Muzeum.

10. W przypadku nieoddania dokumentacji w wyznaczonym terminie, pracownik Archiwum informuje o tym fakcie kierownika jednostki organizacyjnej, której pracownik korzystał z akt. Gdy mimo tego akta nie zostaną zwrócone, powinien zawiadomić dyrektora Muzeum.

VI. WYDZIELANIE I PRZEZNACZANIE DOKUMENTACJI NIEARCHIWALNEJ (KAT. B) NA MAKULATURĘ

1. Pracownik Archiwum planuje na drugie półrocze danego roku wydzielenie dokumentacji ze swojego Archiwum Muzeum.

2. Przez wydzielenie rozumie się:
   a) wyłączenie dokumentacji niearchiwalnej (tj. akt kat. B), której okres przechowywania ustalony według JRWA już minął i przekazaniu jej na makulaturę,
   b) wyłączenie dokumentacji kategorii BE – przeznaczonej do ekspertyzy właściwego Archiwum Państwowego.

3. Wydzielenie dokumentacji odbywa się komisyjnie. W skład komisji wchodzą: zwierzchnik pracownika Archiwum, przedstawiciele komórek organizacyjnych, których akta będą wydzielane oraz pracownik Archiwum. Przy wydzieleniu dokumentacji komisja dokonuje konfrontacji zgodności opisu teczek z ich zawartością.

4. Komisja ma prawo przekwalifikować dokumentację niearchiwalną (akt kat. B) do kategorii A za zgodą właściwego Archiwum Państwowego. Komisja ma także prawo przedłużyć okres przechowywania dokumentacji niearchiwalnej.

5. Po wydzieleniu dokumentacji w Archiwum Muzeum komisja dokonuje zakwalifikowania dokumentacji niearchiwalnej (kat. B) do zniszczenia lub do zmiany kategorii archiwalnej. W tym celu sporządza w dwóch egzemplarzach protokół oceny dokumentacji niearchiwalnej (załącznik nr 6 do niniejszej Instrukcji), której okres przechowywania już upłynął oraz spis dokumentacji niearchiwalnej przeznaczonej na makulaturę lub zniszczenie (załącznik nr 4 lub nr 5 do niniejszej Instrukcji).

6. Wyżej wymienione spisy i protokoły po podpisaniu przez wszystkich członków komisji przedkłada się do akceptacji dyrektora Muzeum.

7. Dwa egzemplarze wymienionego spisu wraz z protokołem przesyła się do Archiwum Państwowego w Katowicach, oddział w Raciborzu, celem uzyskania zgody na dokonanie zniszczenia dokumentacji. Bez tej zgody nie dokonuje się zniszczenia dokumentacji.

8. Archiwum Państwowe w Katowicach, oddział w Raciborzu, wydaje zgodę na dokonanie zniszczenia dokumentacji w dwóch egzemplarzach. Pierwszy dołącza się do spisu wybrakowanej dokumentacji, a drugi służy do przedstawienia w zbiornicy makulatury. Dokumentację przeznaczoną na makulaturę doprowadza się do stanu uniemożliwiającego jej odtworzenie.

9. Archiwum Państwowe w Katowicach, oddział w Raciborzu, może przeprowadzić ekspertyzę dokumentacji uznanej za przeznaczoną do wybrakowania i zażądać przeprowadzenia nowego brakowania. Zmianę kwalifikacji dokumentacji należy odnotować w spisach zdawczo-odbiorczych.

10. Pracownik Archiwum Muzeum po uzyskaniu zgody Archiwum Państwowego w Katowicach, oddział w Raciborzu, i przekazaniu akt do zbiornicy makulatury dokonuje adnotacji o zniszczeniu tych akt w odpowiedniej rubryce spisów zdawczo-odbiorczych.

11. Szczególnie zwraca się uwagę na zachowanie dokumentacji niezbędnej do dalszej pracy jednostki organizacyjnej lub potrzebnej w celach kontrolnych, dowodowych, w sprawach będących w toku postępowania sądowego lub dyscyplinarnego.

VII. OCHRONA INFORMACJI

1. Część dokumentacji związanej z działalnością Muzeum znajdującą się tylko i wyłącznie na magnetycznych nośnikach informacji należy chronić przed utratą, wobec czego niezbędne jest chronienie danych poprzez:
   a) systematyczne sporządzanie kopii (co najmniej dwóch) zabezpieczanych zbiorów na nośnikach niezależnych od systemu (streamery, dyski, dyskietki, CD-ROM-y),
   b) opisanie nośników zawierających kopie zabezpieczanych zbiorów,
   c) przeciwdziałanie utracie danych zawartych na nośnikach oraz zapobieganie skutkom działania wirusów,
   d) prowadzenie ewidencji nośników z zabezpieczanymi danymi.

2. Kopie powinny być przechowywane w miejscu uniemożliwiającym ich fizyczne zniszczenie i dostęp osób niepowołanych (najlepiej w sejfie ogniotrwałym), z daleka od pól magnetycznych, kurzu, zabrudzenia.

VIII. KONTROLA ARCHIWUM MUZEUM

1. Nadzór nad stanem i sposobem przechowywania dokumentacji w Archiwum Muzeum sprawuje Archiwum Zakładowe Urzędu Miasta Żory.
2. Przedstawiciele Archiwum Zakładowego Urzędu Miasta Żory sporządzają protokoły z przeprowadzonych kontroli Archiwum Muzeum i wydają zalecenia pokontrolne, do realizacji których jest zobowiązane Muzeum. Protokół z kontroli Archiwum Muzeum podpisuje dyrektor Muzeum oraz pracownik Archiwum Muzeum.

ZAŁĄCZNIK NR 1

SPIS ZDAWCZO-ODBIORCZY

Muzeum Miejskie

nazwa komórki organizacyjnej .....

Lp.	Znak teczki	Tytuł teczki lub tomu	Daty skrajne od – do	Kat. akt	Liczba teczek	Miejsce przechowywania akt w archiwum	Data zniszczenia lub przekazania
1	2	3	4	5	6	7	8

Rubryki 7 i 8 wypełnia Archiwum MM

....

Przekazująca akta
(podpis)

imię i nazwisko
(czytelnie)
Dyrektor MM
(podpis)

imię i nazwisko
(czytelnie)
Przejmujący akta:
(podpis)

imię i nazwisko
(czytelnie)

ZAŁĄCZNIK NR 2

WYKAZ SPISÓW ZDAWCZO-ODBIORCZYCH

Numer spisu	Data przyjęcia akt	Nazwa komórki przekazującej akta	Liczba		Uwagi
			poz. spisu	teczek	
1	2	3	4	5	6

ZAŁĄCZNIK NR 3

KARTA UDOSTĘPNIENIA AKT

Wykaz spisów zdawczo-odbiorczych

<table>
<tr><td>Komórka organizacyjna</td><td colspan="3">Karta udostępnienia akt nr ..... **)</td></tr>
<tr><td rowspan="2">Data</td><td></td><td>**)</td><td>**)</td></tr>
<tr><td colspan="3">Termin zwrotu akt</td></tr>
<tr><td colspan="4">Proszę o udostępnienie *) – wypożyczenie *) akt powstałych
w komórce organizacyjnej ..... z lat .....
o znakach .....
i upoważniam do ich wykorzystania *) – odbioru *)
Panią / Pana: .....
Imię i Nazwisko
.....
Podpis</td></tr>
<tr><td colspan="4">Zezwalam na udostępnienie *) – wypożyczenie *) wymienionych wyżej akt
.....
Data i podpis
*) Zbędne skreślić **) Wypełnia Archiwum MM</td></tr>
<tr><td colspan="4">Potwierdzam odbiór wymienionych
akt-tomów ..... kart .....
Data: ..... Podpis: .....</td></tr>
<tr><td colspan="4">Adnotacje o zwrocie akt:</td></tr>
<tr><td>Podpis oddającego:
.....</td><td colspan="2">Akta zwrócono do Archiwum MM
Data: .....</td><td>Podpis odbierającego:
.....</td></tr>
</table>

ZAŁĄCZNIK NR 4

SPIS DOKUMENTACJI NIEARCHIWALNEJ (AKTOWEJ) PRZEZNACZONEJ NA MAKULATURĘ LUB ZNISZCZENIE

Nazwa i adres komórki organizacyjnej .....

Spis dokumentacji niearchiwalnej

(aktowej) przeznaczonej na makulaturę lub zniszczenie

Lp.	Nr i lp. spisu zdawczo-odbiorczego	Symbol z wykazu akt	Tytuł teczki	Daty skrajne	Liczba tomów	Uwagi
1	2	3	4	5	6	7

ZAŁĄCZNIK NR 5

SPIS DOKUMENTACJI NIEARCHIWALNEJ (TECHNICZNEJ) PRZEZNACZONEJ NA MAKULATURĘ LUB ZNISZCZENIE

Lp.	Sygn. dok. technicznej	Nazwa obiektu, lokalizacja i tytuły jego projektów	Branża	Stadium	Ilość		Nazwisko projektanta	Data zniszczenia opracowania projektu	Uwagi
					teczek	matryc			
1	2	3	4	5	6	7	8	9	10

ZAŁĄCZNIK NR 6

PROTOKÓŁ OCENY DOKUMENTACJI NIEARCHIWALNEJ

Nazwa i adres komórki organizacyjnej .....

Protokół oceny
dokumentacji nearchiwalnej

Komisja w składzie: (imiona, nazwiska i stanowiska członków Komisji)

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

dokonała oceny i wydzielenia przeznaczonej do przekazania na makulaturę lub zniszczenie dokumentacji niearchiwalnej w ilości ..... mb i stwierdziła, że stanowi ona dokumentację niearchiwalną nieprzydatną dla celów praktycznych jednostki organizacyjnej, oraz że upłynęły terminy jej przechowania określone w Jednolitym rzeczowym wykazie akt lub kwalifikatorze dokumentacji technicznej.

Przewodniczący Komisji .....
Członkowie komisji .....
(podpisy) .....

Załączniki:
..... kart spisu
..... pozycji spisu