Polityka bezpieczeństwa informacji i zarządzania systemem informatycznym Muzeum Miejskie w Jastrzębiu-Zdroju

Spis treści

Polityka bezpieczeństwa informacji i zarządzania systemem informatycznym Muzeum Miejskie w Jastrzębiu-Zdroju 1

1. Cele i zakres polityki 1
2. Klasyfikacja informacji 2
3. Zasady zarządzania dostępem do systemów IT 3
4. Bezpieczeństwo sieci, stacji roboczych i urządzeń 5
5. Procedury tworzenia kopii zapasowych (backup) i ich przechowywania 7
6. Zarządzanie incydentami bezpieczeństwa informacji 9
7. Wymagania wobec dostawców i usług IT (zgodność z RODO, umowy powierzenia) 11
8. Szkolenia i podnoszenie świadomości użytkowników 13
9. Role i odpowiedzialności w zakresie bezpieczeństwa informacji 15

1. Cele i zakres polityki

Celem niniejszej Polityki jest zapewnienie ochrony wszelkich informacji przetwarzanych w Muzeum – w tym danych osobowych i informacji prawnie chronionych – poprzez utrzymanie ich poufności, integralności oraz dostępności. Dokument ten realizuje wymogi art. 24 ust. 2 oraz art. 32 RODO, zobowiązujące administratora do wdrożenia adekwatnych polityk bezpieczeństwa oraz środków technicznych i organizacyjnych. Polityka ma zastosowanie do całej działalności Muzeum (jako publicznej instytucji kultury) i obejmuje wszystkie systemy informatyczne oraz formy przetwarzania informacji – zarówno elektroniczne, jak i papierowe. Zakresem objęci są wszyscy pracownicy, współpracownicy i inne osoby korzystające z zasobów systemu informatycznego Muzeum. Polityka uwzględnia specyfikę muzeum, zgodnie z wytycznymi Urzędu Ochrony Danych Osobowych (UODO) dot. bezpieczeństwa

systemów IT oraz dobrymi praktykami instytucji kultury, które muszą sprostać współczesnym wyzwaniom w obszarze cyberbezpieczeństwa.

Do celów Polityki należy również zapewnienie zgodności z obowiązującymi przepisami (RODO, ustawa o ochronie danych osobowych, ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne itp.) oraz wymaganiami kontraktowymi w zakresie ochrony informacji. Polityka ustanawia jednolite zasady postępowania z informacjami i bezpieczeństwa systemów informatycznych Muzeum. Dokument ten stanowi wewnętrzną regulację, której przestrzeganie jest obowiązkowe dla wszystkich osób związanych z Muzeum – każdy pracownik i współpracownik jest zobowiązany do znajomości i stosowania poniższych zasad.

2. Klasyfikacja informacji

W Muzeum dokonuje się klasyfikacji informacji, aby określić wymagany poziom ochrony dla różnych rodzajów danych. Wyróżnia się następujące kategorie:

- **Informacje publiczne (jawne):** Dane i materiały przeznaczone do powszechnej wiadomości, których ujawnienie nie powoduje szkody. Zaliczają się tu np. treści publikowane na stronie internetowej Muzeum, informacje prasowe, ogólnie dostępne opisy zbiorów eksponowanych publicznie, czy *Biuletyn Informacji Publicznej*.
- **Informacje wewnętrzne:** Dane o charakterze roboczym lub organizacyjnym, przeznaczone do użytku wewnątrz Muzeum. Obejmują one m.in. wewnętrzną korespondencję, notatki służbowe, procedury działania i inne dokumenty, które nie są publicznie dostępne. Dostęp do nich mają wyłącznie upoważnieni pracownicy, a ich ujawnienie osobom postronnym jest zabronione.
- **Informacje poufne (chronione):** Dane wymagające szczególnej ochrony z uwagi na obowiązki prawne lub potencjalne negatywne skutki ich ujawnienia. Do tej kategorii zalicza się w szczególności **dane osobowe** – zarówno pracowników, jak i gości czy kontrahentów – które podlegają ochronie zgodnie z RODO. Są to np. dane kadrowe pracowników, listy uczestników wydarzeń kulturalnych, dane klientów kupujących bilety (jeśli takie są zbierane) oraz nagrania z monitoringu wizyjnego (CCTV) przedstawiające osoby odwiedzające Muzeum. Ponadto za poufne uznaje się **informacje finansowe** Muzeum (np. dokumenty księgowe, sprawozdania finansowe, dane dot. darczyńców i sponsorów) oraz **dokumentację zbiorów muzealnych** zawierającą szczegółowe dane o eksponatach. Dokumentacja zbiorów – np. bazy danych artefaktów, informacje o ich stanie, wartości, miejscach przechowywania czy zabezpieczeniach – wymaga specjalnej ochrony z uwagi na dobro dziedzictwa kulturowego i bezpieczeństwo zbiorów. Ujawnienie tych danych mogłoby naruszyć bezpieczeństwo eksponatów lub interes publiczny, dlatego dostęp do nich mają wyłącznie upoważnione osoby

(m.in. pracownicy działu zbiorów, konserwatorzy, dyrekcja). **Rejestry i dokumentacja zamówień publicznych** oraz umów także są traktowane jako informacje poufne do momentu, w którym zgodnie z przepisami pewne ich elementy muszą zostać upublicznione – np. wyniki postępowań przetargowych. Do kategorii poufnej należą ponadto wszelkie informacje objęte tajemnicą prawnie chronioną (np. tajemnica przedsiębiorstwa kontrahentów, ewentualne informacje niejawne w rozumieniu ustawy o ochronie informacji niejawnych – jeśli takie by wystąpiły w działalności Muzeum).

- **Informacje ściśle poufne:** (ewentualna kategoria najwyższa, opcjonalnie stosowana, jeśli w Muzeum przetwarzane są informacje o krytycznym znaczeniu). Byłyby to dane, do których dostęp ma wyłącznie ścisłe kierownictwo lub wyznaczone osoby, np. hasła do kluczowych systemów, plany systemów zabezpieczeń fizycznych, alarmów, kopie kluczy kryptograficznych, itp. W razie występowania takich informacji, powinny one być odpowiednio oznaczone i przechowywane w sposób szczególnie zabezpieczony (np. sejfy, szyfrowanie).

Każda informacja przetwarzana w Muzeum powinna być oznaczona lub traktowana zgodnie z powyższą klasyfikacją. Dane osobowe stanowią istotną część zasobów informacyjnych – są one przetwarzane wyłącznie w określonych celach związanych z działalnością Muzeum (kadry, obsługa zwiedzających, edukacja, marketing, bezpieczeństwo obiektu – monitoring) i podlegają reżimowi ochrony zgodnie z RODO oraz wewnętrzną **Polityką ochrony danych osobowych**. Informacje finansowe oraz dokumentacja zbiorów muzealnych traktowane są jako wrażliwe z punktu widzenia interesów Muzeum i bezpieczeństwa dziedzictwa; ich nieautoryzowane ujawnienie, utrata lub modyfikacja mogłyby wyrządzić istotne szkody, zatem podlegają wysokim standardom zabezpieczeń.

Dla każdej kategorii informacji określa się wymagany poziom zabezpieczeń oraz zasady dostępu (np. oznaczanie dokumentów klauzulą „Poufne", stosowanie haseł do plików zawierających dane poufne, przechowywanie dokumentów papierowych w zamykanych szafach itp.). Wszyscy pracownicy są szkoleni w zakresie rozróżniania kategorii informacji oraz właściwego postępowania z nimi (patrz punkt 8 Polityki).

3. Zasady zarządzania dostępem do systemów IT

Dostęp do systemów informatycznych Muzeum opiera się na zasadzie **minimalnych uprawnień** – każdy użytkownik otrzymuje wyłącznie takie uprawnienia, jakie są niezbędne do wykonywania jego obowiązków. W Muzeum prowadzony jest **rejestr użytkowników** systemów IT, zawierający spis wszystkich osób posiadających konta dostępu oraz przypisane im role i uprawnienia. Tworzenie nowego konta użytkownika lub nadanie dodatkowych uprawnień wymaga zatwierdzenia przez kierownictwo (Dyrektora lub upoważnionego Administratora Systemów Informatycznych) i odbywa się na

zasadzie pisemnego lub mailowego wniosku, dokumentującego zakres dostępu i jego uzasadnienie.

Każdy użytkownik systemu informatycznego otrzymuje **indywidualne konto** (login) oraz hasło. Zabronione jest współdzielenie kont lub przekazywanie swojego hasła innym osobom. Hasła muszą spełniać ustalone wymagania złożoności – co najmniej określoną minimalną długość (np. 8–10 znaków), zawierać kombinację liter, cyfr oraz znaków specjalnych – i nie mogą być łatwe do odgadnięcia (np. brak słów słownikowych czy danych osobowych użytkownika). Nowo utworzone konta są zabezpieczane hasłem startowym, które użytkownik jest zobowiązany zmienić przy pierwszym logowaniu. Wdrożona jest **polityka haseł**, zgodnie z którą hasła należy zmieniać regularnie (np. co 90 dni) oraz nie wolno używać ponownie ostatnich kilku haseł. Systemy informatyczne wymuszają te zasady technicznie, o ile to możliwe (np. wymóg zmiany hasła po upływie terminu, blokada prostych haseł).

Zasady zarządzania kontami obejmują również **blokowanie nieaktywnych kont**. Konta użytkowników, którzy zakończyli współpracę z Muzeum (np. ustanie stosunku pracy) lub którzy nie logowali się przez dłuższy okres, są niezwłocznie dezaktywowane lub usuwane. Procedura zwalniania pracownika obejmuje powiadomienie Administratora Systemów o konieczności zamknięcia lub zawieszenia dostępu danej osoby do systemów (od dnia ustania uprawnień). Okresowo (np. raz na kwartał) dokonywany jest przegląd istniejących kont i uprawnień, celem weryfikacji, czy nie ma zbędnych lub nadmiernych dostępów – w ramach **kontroli dostępu** usuwa się lub koryguje wszystkie nieuzasadnione uprawnienia.

Konto użytkownika jest zabezpieczone przed atakami odgadnięcia hasła poprzez mechanizmy blokady po kilkukrotnej nieudanej próbie logowania (np. trzykrotne błędne hasło powoduje tymczasowe zablokowanie konta). W miarę możliwości wykorzystywane są także mechanizmy **uwierzytelniania dwuskładnikowego (MFA)** – zwłaszcza dla kont administratorów lub dostępu zdalnego – aby dodatkowo zabezpieczyć dostęp do kluczowych systemów.

Przyznawanie uprawnień administracyjnych (np. konta z prawami administratora systemu, dostępy do serwerów, baz danych czy paneli administracyjnych aplikacji) jest ściśle ograniczone do minimalnej liczby osób pełniących funkcje techniczne. Administratorzy systemów są zobowiązani używać kont uprzywilejowanych wyłącznie do zadań administracyjnych; do zwykłej pracy powinny służyć im osobne konta o uprawnieniach użytkownika. Każde nadanie, zmiana lub odebranie uprawnień administracyjnych jest odnotowywane i podlega zatwierdzeniu przez Dyrektora lub osobę przez niego upoważnioną.

Dla zachowania rozliczalności działań w systemach IT, w miarę dostępnych funkcjonalności aktywowane są **mechanizmy rejestrowania logów** (dzienników zdarzeń) – np. rejestrowane są operacje logowania, błędne próby logowania, istotne

akcje administracyjne. Logi te są przechowywane w bezpieczny sposób przez określony czas i podlegają przeglądowi w razie podejrzenia naruszenia bezpieczeństwa.

4. Bezpieczeństwo sieci, stacji roboczych i urządzeń

Muzeum utrzymuje infrastrukturę teleinformatyczną w sposób zapewniający ochronę przed nieautoryzowanym dostępem z zewnątrz, złośliwym oprogramowaniem oraz innymi zagrożeniami. W szczególności wdrożone zostały następujące środki techniczne i organizacyjne:

- **Zabezpieczenia sieciowe (firewall):** Dostęp do sieci Muzeum od strony Internetu jest chroniony poprzez zaporę sieciową (firewall), która filtruje ruch przychodzący i wychodzący. Firewall jest skonfigurowany tak, by blokować nieautoryzowane połączenia oraz potencjalnie niebezpieczne usługi, dopuszczając jedynie ruch niezbędny do funkcjonowania udostępnianych usług (np. strony internetowej Muzeum, poczty elektronicznej, zdalnego dostępu dla upoważnionych osób). Sieć wewnętrzna jest podzielona na segmenty (VLANy) oddzielające przynajmniej strefę dla systemów administracyjnych (wewnętrznych) od sieci dostępnej dla odwiedzających (np. publicznej sieci Wi-Fi dla gości muzeum). Pozwala to zminimalizować ryzyko, że osoba nieuprawniona lub urządzenie gościa uzyska dostęp do wrażliwych zasobów wewnętrznych.
- **Aktualizacje oprogramowania:** Wszystkie serwery, komputery stacjonarne i przenośne oraz inne urządzenia aktywne w sieci (np. routery, kamery systemu monitoringu) są objęte polityką regularnych aktualizacji. Oprogramowanie systemowe (systemy operacyjne) oraz zainstalowane aplikacje muszą być na bieżąco aktualizowane w celu eliminacji znanych luk bezpieczeństwa. Zaniedbanie aktualizacji stanowi poważne ryzyko, gdyż przestarzałe systemy mogą zawierać podatności łatwe do wykorzystania przez wirusy lub ataki typu malware. Dlatego Muzeum wdraża mechanizmy automatycznych aktualizacji tam, gdzie to możliwe lub ustanawia procedurę cyklicznych przeglądów i ręcznej instalacji poprawek (np. comiesięczne „wtorki aktualizacji” dla systemów Microsoft). W razie wydania krytycznej poprawki bezpieczeństwa administrator stara się zastosować ją niezwłocznie, by zminimalizować okno podatności.
- **Oprogramowanie antywirusowe i antymalware:** Wszystkie stacje robocze użytkowników oraz serwery posiadają zainstalowane i aktywne oprogramowanie antywirusowe (AV) z funkcją bieżącej ochrony w czasie rzeczywistym. Programy te są tak skonfigurowane, by regularnie skanowały pliki i pocztę e-mail, wykrywając i usuwając wirusy, trojany, spyware i inne złośliwe komponenty. Bazy wirusów i sygnatur zagrożeń są aktualizowane automatycznie (często nawet codziennie). Pracownicy są zobowiązani do nieignorowania alertów antywirusa i niezwłocznego zgłaszania do Administratora Systemów każdego wykrytego

zagrożenia, którego nie da się automatycznie usunąć. Oprócz antywirusa, stosowane są dodatkowe mechanizmy bezpieczeństwa punktów końcowych, takie jak zapora systemowa na stacjach roboczych, filtrowanie poczty spam/phishing na serwerze pocztowym oraz opcjonalnie *endpoint detection and response* (EDR) – jeżeli środki na to pozwalają – w celu zaawansowanego wykrywania podejrzanych zachowań na urządzeniach.

- **Polityka korzystania z urządzeń i oprogramowania:** W Muzeum obowiązuje zakaz instalowania nieautoryzowanego oprogramowania na służbowych komputerach. Wszelkie programy muszą posiadać licencje i być zatwierdzone przez Administratora Systemów przed instalacją. Użytkownicy nie powinni podłączać prywatnych urządzeń USB, dysków zewnętrznych czy smartfonów do komputerów służbowych bez zgody – wyjątkiem są nośniki zweryfikowane pod kątem braku złośliwego oprogramowania. W razie potrzeby przenoszenia danych na zewnętrznych nośnikach stosuje się ich szyfrowanie lub zabezpieczanie hasłem. Dostęp zdalny do zasobów Muzeum (np. przez VPN) jest ograniczony do upoważnionych pracowników i zabezpieczony odpowiednimi mechanizmami (szyfrowanie połączenia, uwierzytelnienie wieloskładnikowe).
- **Bezpieczeństwo stacji roboczych:** Każdy komputer używany w Muzeum posiada wygaszacz ekranu lub blokadę, która uruchamia się automatycznie po kilku minutach bezczynności, wymagając ponownego zalogowania. Pracownicy są szkoleni, by opuszczając stanowisko choćby na chwilę, blokować swoje komputery (np. skrótem klawiszowym). Dostęp do ustawień systemowych zwykłych użytkowników jest ograniczony – standardowe konta nie mają uprawnień administratora na lokalnych maszynach, aby zapobiec przypadkowemu lub celowemu wprowadzeniu zmian osłabiających zabezpieczenia. Na laptopach stosowane są dodatkowe zabezpieczenia, takie jak szyfrowanie całego dysku (BitLocker lub równoważne) – w przypadku kradzieży urządzenia uniemożliwia to odczyt przechowywanych na nim danych. Urządzenia przenośne zawierające wrażliwe dane (np. laptopy, smartfony służbowe zsynchronizowane z pocztą) posiadają rozwiązania zdalnego zarządzania, pozwalające w razie potrzeby na zdalne wymazanie danych (remote wipe) lub zlokalizowanie sprzętu.
- **Bezpieczeństwo serwerów i pomieszczeń technicznych:** Serwery oraz urządzenia sieciowe (np. switch, NAS) znajdują się w pomieszczeniach zabezpieczonych przed dostępem osób niepowołanych (np. dedykowana serwerownia lub szafa teleinformatyczna zamykana na klucz; dostęp tylko dla Administratora Systemów i Dyrektora). Pomieszczenia te są wyposażone w systemy przeciwpożarowe (gaśnice, czujniki dymu) oraz – o ile to możliwe – w rozwiązania kontroli środowiska (klimatyzacja dla utrzymania odpowiedniej

temperatury urządzeń). Serwery posiadają konta administratorów chronione silnymi hasłami, a dostęp do nich (fizycznie i zdalnie) jest ściśle kontrolowany. Wykonuje się okresowe **testy bezpieczeństwa** infrastruktury (np. skanowanie podatności, testy penetracyjne aplikacji webowych) albo korzysta z zewnętrznych audytów, aby wykryć i usunąć ewentualne słabości systemu zanim zostaną wykorzystane przez osoby trzecie.

- **Monitoring i system alarmowy:** System monitoringu wizyjnego (CCTV) Muzeum stanowi również element bezpieczeństwa informacji (chroni zasoby przed fizyczną ingerencją). Kamery rejestrujące obraz są zainstalowane w sposób zgodny z przepisami (monitorowane strefy są oznaczone, a klauzule informacyjne RODO dot. monitoringu dostępne dla gości). Rejestratory cyfrowe przechowują nagrania przez określony przepisami lub wewnętrznie ustalony czas (np. 14 lub 30 dni), po czym zapis jest nadpisywany automatycznie. Dostęp do nagrań mają wyłącznie upoważnieni pracownicy (np. Dyrektor, wyznaczony pracownik ochrony czy Administrator Systemów) i tylko w uzasadnionych celach (np. wyjaśnienie incydentu bezpieczeństwa). Systemy monitoringu są chronione hasłem, a sieć wykorzystywana przez kamery jest odseparowana od sieci biurowej. Muzeum posiada również system alarmowy chroniący budynek poza godzinami pracy, z powiadomieniem odpowiednich służb (policja, firma ochroniarska) – te środki pośrednio także wspierają ochronę integralności i dostępności systemów informatycznych, minimalizując ryzyko fizycznego zniszczenia lub kradzieży sprzętu.
- **Systemy wykrywania intruzów i monitoring aktywności:** Dążąc do zgodności z najnowszymi wytycznymi bezpieczeństwa (np. dyrektywa NIS2 dla sektora publicznego), Muzeum rozważa wdrożenie systemów wykrywania włamań (IDS/IPS) oraz centralnego monitoringu sieci. Regularne aktualizacje i monitorowanie anomalii w ruchu sieciowym są coraz częściej wymagane dla zapewnienia wysokiego poziomu ochrony. Stały nadzór nad infrastrukturą umożliwia wczesne wychwycenie symptomów ataku lub awarii, co pozwala podjąć szybkie działania zapobiegawcze (np. zablokowanie nietypowego ruchu sieciowego mogącego wskazywać na próbę wykradania danych).

5. Procedury tworzenia kopii zapasowych (backup) i ich przechowywania

Muzeum utrzymuje systematyczne procedury wykonywania kopii zapasowych kluczowych danych i systemów, aby zapewnić możliwość odtworzenia danych w razie awarii, ataku ransomware lub innego zdarzenia skutkującego utratą dostępu do informacji. **Dane cyfrowe stanowią bezcenny zasób Muzeum** – obejmują m.in. katalogi zbiorów (digitalizowana ewidencja eksponatów), archiwalne materiały fotograficzne, dokumentację działalności, a także informacje o zwiedzających

(rezerwacje biletów, listy mailingowe, dane darczyńców itp.). Utrata tych danych byłaby katastrofalna w skutkach dla ciągłości działania i dziedzictwa kulturowego, stąd regularny backup jest absolutną koniecznością. Niestety, jak pokazują statystyki, aż 70% małych organizacji w Polsce nie wykonuje regularnych kopii zapasowych, często w błędnym przeświadczeniu „nas to nie spotka". Muzeum Miejskie w Jastrzębiu-Zdroju unika tego błędu poprzez wdrożenie rygorystycznej polityki backupu.

Harmonogram kopii zapasowych: Dla serwerów i baz danych (np. baza kolekcji, baza księgowa, system kadrowy) wykonywane są pełne kopie zapasowe przynajmniej raz w tygodniu, zaś inkrementacyjne (differentialne) kopie – codziennie w dni robocze. Dane na stacjach roboczych użytkowników (dokumenty) powinny być przechowywane na serwerze sieciowym lub w usłudze typu NAS, która również jest objęta backupem, zamiast jedynie na dysku lokalnym. Kopie zapasowe obejmują także konfiguracje kluczowych urządzeń (np. eksport konfiguracji routera, ustawień systemów alarmowych, itp.).

Przechowywanie kopii: Kopie zapasowe przechowywane są w dwóch formach – **online i offline**. Backup online to bieżąca kopia utrzymywana na zasobie sieciowym (np. na serwerze backupów lub macierzy dyskowej w innej części budynku), co umożliwia szybkie przywrócenie danych w razie typowej awarii systemu. Ponadto, regularnie tworzone są **kopie offline (archiwalne)** – np. na nośnikach wymiennych (dyski zewnętrzne, taśmy LTO) – które po wykonaniu są odłączane od systemu i przechowywane w bezpiecznej lokalizacji (np. w sejfie przeciwpożarowym w innym pomieszczeniu, a idealnie – poza siedzibą Muzeum). Taka praktyka chroni przed utratą danych wskutek złośliwego ataku (np. ransomware szyfrującego także dostępne kopie online) czy zdarzeń losowych w obiekcie (pożar, zalanie).

Cykl wymiany i retencja: Nośniki z kopiami offline są używane rotacyjnie – np. w systemie tygodniowym z co najmniej dwoma kompletami nośników (aby zawsze jedna kopia znajdowała się fizycznie poza głównym systemem). Kopie zapasowe są przechowywane przez określony okres (retencja), np. dzienne przyrostowe – 1 tydzień, tygodniowe pełne – 1 miesiąc, comiesięczne archiwalne – 6 miesięcy lub dłużej, w zależności od potrzeb i przestrzeni. Po upływie okresu retencji starsze kopie są bezpiecznie niszczone lub nadpisywane, o ile nie zachodzi potrzeba ich dłuższego przechowania (np. ze względu na przepisy archiwizacyjne).

Testy odtwarzania: Sama obecność kopii nie gwarantuje bezpieczeństwa – równie ważna jest umiejętność i możliwość odtworzenia danych. Dlatego Muzeum regularnie testuje procedurę **przywracania kopii zapasowych**. Przynajmniej raz na kwartał przeprowadzany jest test polegający na odtworzeniu wybranego fragmentu danych lub całego systemu z backupu (np. odtworzenie wybranej bazy danych na serwerze testowym). Pozwala to zweryfikować, czy kopie są prawidłowo wykonywane i spójne oraz czy instrukcje odtworzeniowe są kompletne. Wyniki testów są dokumentowane.

Bezpieczeństwo kopii zapasowych: Dostęp do miejsc przechowywania kopii zapasowych mają tylko upoważnione osoby (Administrator Systemów oraz ewentualnie Dyrektor). Kopie zawierające dane wrażliwe (np. dane osobowe) są dodatkowo zabezpieczane – nośniki są zaszyfrowane lub chronione hasłem, co uniemożliwia odczyt danych przez niepowołane osoby w razie zagubienia czy kradzieży nośnika. Nośniki z backupami są oznaczane, ewidencjonowane i przechowywane w warunkach zabezpieczających je przed zniszczeniem (np. w pojemniku ognioodpornym).

Ścisłe przestrzeganie powyższych procedur backupu ma krytyczne znaczenie dla ciągłości działania Muzeum. Przykłady z niedawnej przeszłości pokazują dotkliwe skutki zaniedbań w tym zakresie – np. podczas ataku ransomware na systemy Urzędu w Krakowie okazało się, że ostatnia dostępna sprawna kopia zapasowa miała kilka dni, co przy braku nowszych backupów doprowadziło do utraty danych i operacyjnego chaosu. Brak aktualnych kopii zapasowych oznacza realne ryzyko nieodwracalnej utraty danych oraz długotrwałego paraliżu działalności. Muzeum Miejskie w Jastrzębiu-Zdroju uczyniło więc z backupu priorytet, dbając by w żadnym momencie luka czasowa między kopiami nie była na tyle duża, by zagrozić cennym zasobom informacyjnym.

6. Zarządzanie incydentami bezpieczeństwa informacji

Incydentem bezpieczeństwa informacji jest każde zdarzenie, które stanowi zagrożenie dla poufności, integralności lub dostępności informacji bądź systemów informatycznych Muzeum. Może to być m.in. wykrycie złośliwego oprogramowania na komputerze, nieautoryzowana próba dostępu do systemu, naruszenie ochrony danych osobowych (np. ujawnienie lub utrata nośnika z danymi), awaria sprzętu skutkująca utratą danych, czy atak hakerski (phishing, ransomware, DoS itp.). Każdy pracownik Muzeum ma obowiązek niezwłocznie **zgłaszać** zauważony incydent lub podejrzenie incydentu osobie odpowiedzialnej – przede wszystkim Administratorowi Systemów Informatycznych oraz (jeśli incydent dotyczy danych osobowych) Inspektorowi Ochrony Danych. Zgłoszenie powinno nastąpić natychmiast po wykryciu problemu, bez zatajania czy samodzielnego próbowania rozwiązania, które mogłoby utrudnić analizę śladów.

Po otrzymaniu zgłoszenia incydentu uruchamiana jest procedura **reakcji na incydent**, obejmująca następujące etapy:

1. **Identyfikacja i ocena incydentu:** Zespół odpowiedzialny (Administrator Systemów, IOD, ewentualnie Dyrektor) zbiera informacje o zdarzeniu, aby potwierdzić czy rzeczywiście doszło do incydentu, jakiego rodzaju i jakiego zakresu danych lub systemów dotyczy. Następnie ocenia się wstępnie skalę i potencjalny wpływ incydentu (czy dotyczy danych osobowych, ilu osób, jakich systemów, czy incydent trwa nadal).
2. **Ograniczenie szkód (powstrzymanie incydentu):** Podejmowane są niezwłocznie działania, by zminimalizować skutki. W zależności od sytuacji może

to oznaczać odłączenie zainfekowanej stacji od sieci, zablokowanie konta, zmiana haseł, wyłączenie zaatakowanego serwera, uruchomienie zapasowego systemu itp. Priorytetem jest powstrzymanie dalszego „wycieku" informacji lub rozprzestrzeniania się zagrożenia.

3. **Usunięcie przyczyny:** Po opanowaniu sytuacji analizuje się źródło incydentu i podejmuje działania naprawcze – np. usunięcie malware z systemu, załatanie podatności (instalacja aktualizacji bezpieczeństwa), korekta konfiguracji zabezpieczeń, naprawa lub wymiana uszkodzonego sprzętu. W razie potrzeby korzysta się z pomocy zewnętrznych ekspertów (np. firma informatyczna, która przeprowadzi analizę śledczą czy odtworzy dane).

4. **Odtworzenie działania:** Przywracane są utracone dane i funkcjonalności systemów, aby Muzeum mogło jak najszybciej wrócić do normalnej pracy. Wykorzystuje się do tego ostatnie dostępne kopie zapasowe (zgodnie z procedurą backup). Sprawdza się integralność odtworzonych danych i poprawność działania systemów po incydencie.

5. **Analiza post-incident i wnioski:** Po zakończeniu incydentu zespół dokonuje pełnej analizy przyczyn i przebiegu zdarzenia. Tworzony jest raport z incydentu, opisujący co się stało, jakie działania podjęto, jakie były straty lub skutki oraz rekomendacje na przyszłość. Raport ten jest archiwizowany w **Rejestrze incydentów bezpieczeństwa informacji**. Na podstawie wniosków wdrażane są usprawnienia, by zapobiec podobnym incydentom – np. dodatkowe szkolenie pracowników, zmiana procedur, wprowadzenie nowych zabezpieczeń.

Naruszenia ochrony danych osobowych: Jeżeli incydent dotyczy danych osobowych i spełnia kryteria **naruszenia ochrony danych** w rozumieniu RODO (np. prowadzi do przypadkowego lub nieuprawnionego zniszczenia, utraty, zmodyfikowania, ujawnienia bądź dostępu do danych osobowych), Muzeum realizuje dodatkowe czynności zgodne z art. 33 i 34 RODO. W szczególności Inspektor Ochrony Danych dokonuje oceny ryzyka dla praw i wolności osób fizycznych wynikającego z zaistniałego incydentu. Jeśli istnieje prawdopodobieństwo, że naruszenie może skutkować takim ryzykiem, **zgłaszamy naruszenie do Prezesa UODO** niezwłocznie – najlepiej w ciągu 72 godzin od stwierdzenia incydentu. Zgłoszenie obejmuje opis naruszenia, kategorie i szacunkową liczbę osób, których dotyczy, oraz podjęte środki zaradcze. W przypadku gdy naruszenie może powodować wysokie ryzyko negatywnych konsekwencji dla osób fizycznych (np. ujawniono dane wrażliwe), Muzeum **informuje również te osoby** o incydencie, przekazując im zalecenia co do ochrony przed skutkami (zgodnie z art. 34 RODO). Wszystkie naruszenia danych osobowych, niezależnie od obowiązku zgłoszenia do UODO, są odnotowywane w wewnętrznym **Rejestrze naruszeń ochrony danych** (prowadzonym na podstawie art. 33 ust. 5 RODO).

Zgłaszanie incydentów z obszaru cyberbezpieczeństwa: Choć Muzeum nie jest bezpośrednio objęte ustawowym obowiązkiem zgłaszania incydentów do organów takich jak CSIRT (Computer Security Incident Response Team) – instytucje kultury formalnie nie należą obecnie do katalogu podmiotów kluczowych z ustawy o krajowym systemie cyberbezpieczeństwa – przyjęto zasadę, że poważne incydenty (zwłaszcza ataki cybernetyczne) mogą być zgłaszane odpowiednim służbom w celu szerszej analizy i ostrzeżenia innych podmiotów. W przypadku np. ataku phishingowego, który mógłby dotknąć inne instytucje, czy powtarzających się prób włamań, Administrator Systemów lub IOD może dokonać zgłoszenia incydentu do zespołu reagowania na incydenty (np. CERT Polska) poprzez platformę incydent.cert.pl. Takie działanie, choć nieobowiązkowe, jest rekomendowane w duchu współpracy na rzecz zwiększenia bezpieczeństwa całego sektora kultury.

Pracownicy Muzeum są zachęcani do **pełnej otwartości w zgłaszaniu incydentów i słabości** – incydent nie jest powodem do karania zgłaszającego (o ile nie wynika z rażącego naruszenia obowiązków), a rzetelne informacje pozwalają lepiej zabezpieczyć organizację. Stworzono klimat, w którym bezpieczeństwo jest priorytetem i ważniejsze od unikania przyznania się do błędu. Procedury incydentowe są regularnie aktualizowane i testowane (np. poprzez ćwiczenia symulacyjne), aby w sytuacji kryzysowej personel wiedział, jak reagować.

7. Wymagania wobec dostawców i usług IT (zgodność z RODO, umowy powierzenia)

Muzeum korzysta z usług zewnętrznych dostawców w zakresie wsparcia IT oraz innych usług, co często wiąże się z dostępem tych podmiotów do informacji Muzeum (w tym danych osobowych). W celu zapewnienia bezpieczeństwa na każdym etapie przetwarzania danych, Muzeum stosuje zasadę, że **każdy dostawca lub usługodawca**, który w ramach realizacji umowy może przetwarzać dane Muzeum, musi spełniać określone wymagania bezpieczeństwa oraz (jeśli dotyczy to danych osobowych) zawrzeć stosowną **umowę powierzenia przetwarzania danych** zgodnie z art. 28 RODO.

Przed nawiązaniem współpracy z dostawcą IT lub innym podmiotem, któremu potencjalnie powierzone zostaną dane, Muzeum dokonuje **weryfikacji podmiotu przetwarzającego**. Sprawdza się, czy dany podmiot daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych w celu ochrony danych oraz zapewnienia zgodności przetwarzania z RODO. W praktyce oznacza to np.: żądanie od dostawcy informacji o posiadanych certyfikatach bezpieczeństwa (typu ISO 27001), opis stosowanych zabezpieczeń (polityki bezpieczeństwa, szyfrowanie, systemy kontroli dostępu), a także analizę jego reputacji i doświadczenia. Dopiero pozytywna ocena pozwala na powierzenie danych. Brak takiej weryfikacji i umowy powierzenia może skutkować sankcjami – przykład stanowi ukarana przez UODO instytucja kultury,

która zlecała usługi księgowe bez umowy powierzenia i bez upewnienia się, że wykonawca spełnia wymogi bezpieczeństwa.

Z każdym dostawcą, któremu przekazywane są dane osobowe (np. firma serwisująca system informatyczny, dostawca usługi chmury do archiwizacji danych, operator systemu sprzedaży biletów online, firma obsługująca newsletter lub system monitoringu), Muzeum zawiera pisemną **umowę powierzenia przetwarzania danych**. Umowa taka określa m.in. zakres i cel powierzonego przetwarzania, rodzaj danych i kategorie osób, obowiązki dostawcy w zakresie poufności, zabezpieczenia danych, wsparcia administratora w realizacji obowiązków (np. pomoc w odpowiadaniu na żądania osób, których dane dotyczą, pomoc przy incydentach), warunki podpowierzenia ewentualnego (czy może angażować podwykonawców) oraz zasady postępowania z danymi po zakończeniu współpracy (zwrot lub usunięcie danych). Podmiot przetwarzający zobowiązany jest działać wyłącznie na udokumentowane polecenie Muzeum oraz umożliwić Muzeum przeprowadzanie kontroli zgodności z postanowieniami umowy (audit bezpieczeństwa).

W treści umów z dostawcami zawierane są **klauzule poufności** – wykonawca i jego personel muszą zobowiązać się do zachowania w tajemnicy wszelkich informacji uzyskanych od Muzeum, w tym danych osobowych i informacji o zabezpieczeniach systemu. W razie stwierdzenia przez Muzeum uchybień w zabezpieczeniach po stronie dostawcy lub przypadku incydentu z jego winy, umowa przewiduje możliwość żądania podjęcia stosownych działań naprawczych, a nawet rozwiązania współpracy.

Dostawcy IT mają obowiązek **niezwłocznie zgłaszać** Muzeum każdy incydent bezpieczeństwa dotyczący powierzonych im danych (np. włamanie do systemu dostawcy, które mogło objąć dane Muzeum). Ponadto Muzeum wymaga od nich, by zapewnili sobie podobne zobowiązania od ewentualnych dalszych podwykonawców (podpowierzenie danych wymaga zgody Muzeum i równych gwarancji bezpieczeństwa na kolejnych poziomach).

W ramach zarządzania relacjami z dostawcami, Muzeum prowadzi **ewidencję umów powierzenia** i okresowo ją przegląda. Inspektor Ochrony Danych, we współpracy z Administratorem Systemów, może dokonywać przeglądu stanu zabezpieczeń u kluczowych dostawców (np. poprzez ankiety bezpieczeństwa, żądanie raportów z testów penetracyjnych czy audytów, wizyty kontrolne, jeśli to uzasadnione). Jeżeli dostawca przetwarza dane osobowe obywateli Unii poza EOG, Muzeum upewnia się, że spełnione są dodatkowe wymogi prawne (np. standardowe klauzule umowne przy transferze danych).

Dzięki powyższym działaniom Muzeum minimalizuje ryzyko związane z przekazywaniem danych na zewnątrz. Współpracuje wyłącznie z tymi partnerami, którzy podchodzą poważnie do kwestii ochrony danych i potrafią to wykazać konkretnymi środkami. W razie wątpliwości co do bezpieczeństwa oferowanego przez potencjalnego wykonawcę,

Muzeum rezygnuje z powierzenia mu informacji wrażliwych lub stawia dodatkowe warunki zabezpieczające.

8. Szkolenia i podnoszenie świadomości użytkowników

Czynnik ludzki jest często najsłabszym ogniwem w łańcuchu bezpieczeństwa, dlatego Muzeum przykłada dużą wagę do regularnych szkoleń i budowania kultury bezpieczeństwa informacji wśród pracowników. Bez właściwego przeszkolenia pracownicy mogą nieświadomie stać się „słabym punktem", przez który atakujący uzyskają dostęp do cennych danych i systemów. Z tego względu wdrożono następujące zasady w zakresie edukacji i świadomości:

- **Szkolenie wstępne:** Każda nowo zatrudniona osoba (lub nowy współpracownik) przed dopuszczeniem do pracy z systemami informatycznymi przechodzi szkolenie z zasad bezpieczeństwa informacji i ochrony danych osobowych obowiązujących w Muzeum. Szkolenie to obejmuje zapoznanie z niniejszą Polityką, procedurami dotyczącymi haseł, korzystania z poczty elektronicznej, Internetu, zasadami klasyfikacji informacji, reagowania na incydenty, a także podstawowymi obowiązkami wynikającymi z RODO. Nowy pracownik potwierdza pisemnie (lub elektronicznie) zapoznanie się z zasadami ochrony informacji oraz zobowiązanie do ich przestrzegania.
- **Regularne szkolenia okresowe:** Co najmniej raz w roku organizowane są dla całego personelu odświeżające szkolenia lub warsztaty z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa. Na szkoleniach tych omawiane są aktualne zagrożenia (np. nowe metody phishingu, ataki socjotechniczne, złośliwe oprogramowanie), przypominane są zasady polityki, a także prezentowane ewentualne incydenty, które wydarzyły się w ostatnim czasie (w Muzeum lub w podobnych instytucjach) wraz z wnioskami. Celem jest utrzymanie wysokiej świadomości ryzyka – pracownicy powinni wiedzieć, na co zwracać uwagę i jak reagować. Szkolenia uwzględniają poziom wiedzy odbiorców – inne akcenty mogą być dla zespołu IT, a inne dla pracowników merytorycznych, jednak wszyscy muszą rozumieć podstawowe zasady (jak chronić hasło, jak rozpoznać podejrzany e-mail, co jest dopuszczalne w korzystaniu z danych osobowych, itp.). Wiele przepisów (w tym RODO) wymaga wdrożenia takich środków jak szkolenia pracowników, co dodatkowo motywuje Muzeum do ich prowadzenia.
- **Uświadamianie na co dzień:** Oprócz formalnych szkoleń, Muzeum dba o utrzymanie tematu bezpieczeństwa w codziennej świadomości pracowników. Wykorzystuje się do tego np. komunikaty e-mailowe przypominające o zasadach (zwłaszcza przy obserwacji wzmożonych prób ataków, np. ostrzeżenie „uwaga na podejrzane maile zatytułowane X"), plakaty lub infografiki w przestrzeni biurowej

(np. przy stanowiskach pracy – „Czy zablokowałeś komputer odchodząc od biurka?"), okazjonalne testy socjotechniczne (kontrolowane próby phishingu wysyłane do pracowników, by sprawdzić ich czujność i wyciągnąć wnioski szkoleniowe).

- **Polityka czystego biurka i ekranu:** W ramach kształtowania dobrych nawyków informacyjnych obowiązuje zasada czystego biurka – pracownicy nie zostawiają na wierzchu dokumentów papierowych zawierających dane poufne po zakończeniu pracy; wszystko powinno być schowane w szafkach zamykanych na klucz. Analogicznie – polityka czystego ekranu wymaga, by nie zostawiać na ekranie komputera otwartych niezaszyfrowanych plików z danymi poufnymi, gdy nie są już potrzebne oraz by wylogowywać się z systemów po zakończeniu pracy. Kierownictwo oraz IOD przeprowadzają nieformalnie od czasu do czasu obchód kontrolny, by ocenić przestrzeganie tych zasad, a ewentualne uchybienia są omawiane z pracownikami (celem edukacji, nie represji).
- **Świadomość odpowiedzialności:** Pracownicy są informowani o konsekwencjach naruszenia zasad bezpieczeństwa. Dotyczy to zarówno potencjalnych zagrożeń dla Muzeum (utrata danych, szkody finansowe i wizerunkowe, sankcje prawne), jak i konsekwencji personalnych (od odpowiedzialności dyscyplinarnej, poprzez cywilną, aż po ewentualną odpowiedzialność karną w przypadku umyślnego naruszenia np. tajemnicy). Komunikowane jest jednak, że celem Polityki nie jest karanie, lecz zapobieganie – stąd większy nacisk kładzie się na zachęcanie do ostrożności i natychmiastowego zgłaszania błędów (nawet własnych) niż na represje.
- **Specjalistyczne szkolenia:** Osoby pełniące szczególne role (np. Administrator Systemów, IOD, administrator bazy zbiorów) uczestniczą w dodatkowych szkoleniach z zakresu swoich obowiązków. Administratorzy IT szkolą się z nowych technologii zabezpieczeń, metod wykrywania ataków, procedur ciągłości działania. IOD regularnie podnosi kwalifikacje z zakresu przepisów o ochronie danych i praktyki UODO. Wiedza z takich szkoleń jest następnie przekazywana wewnętrznie i wykorzystywana do ulepszania Polityki oraz procedur.

Budowanie kultury bezpieczeństwa, w której każdy czuje się odpowiedzialny za ochronę informacji, jest nadrzędnym celem tych działań. Dąży się do tego, by bezpieczeństwo było postrzegane jako wartość wspólna całej organizacji, a nie tylko „sprawa działu IT". Pracownicy rozumieją, że stosowanie zasad bezpieczeństwa nie jest biurokratyczną fanaberią, ale realnie chroni zarówno Muzeum, jak i ich samych. Inwestycja w edukację cyber bezpieczeństwa przekłada się na zmniejszenie liczby incydentów (wiele naruszeń wynika z ludzkich błędów, którym można zapobiec szkoleniem) oraz zwiększa zaufanie otoczenia do instytucji. Klienci, darczyńcy i partnerzy mają większe zaufanie do

Muzeum, wiedząc, że ich dane są bezpieczne i że organizacja przykłada wagę do ich ochrony.

9. Role i odpowiedzialności w zakresie bezpieczeństwa informacji

Za wdrożenie i utrzymanie Polityki bezpieczeństwa informacji odpowiada kierownictwo Muzeum, przy wsparciu wyznaczonych funkcjonariuszy. Role oraz zakresy odpowiedzialności przedstawiają się następująco:

- **Administrator Danych Osobowych (ADO)** – w przypadku Muzeum publicznego funkcję Administratora pełni Muzeum reprezentowane przez **Dyrektora Muzeum**. Dyrektor ponosi ogólną odpowiedzialność za zapewnienie zgodności przetwarzania danych z prawem oraz za bezpieczeństwo informacji w jednostce. Do jego zadań należy zatwierdzanie niniejszej Polityki i wszelkich powiązanych procedur, zapewnienie zasobów (personalnych, finansowych, technicznych) na wdrożenie wymaganych zabezpieczeń oraz nadzór nad przestrzeganiem ustalonych zasad. Dyrektor wspiera działalność Inspektora Ochrony Danych i Administratora Systemów poprzez autorytet w egzekwowaniu przepisów oraz podejmowanie decyzji strategicznych (np. akceptacja poziomu ryzyka rezydualnego, decyzje o zgłoszeniu naruszenia do UODO w konsultacji z IOD itp.).
- **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona zgodnie z art. 37 RODO, odpowiedzialna za monitorowanie przestrzegania przepisów o ochronie danych osobowych w Muzeum. IOD pełni funkcję doradczą i kontrolną: opiniuje wewnętrzne regulacje (takie jak niniejsza Polityka) pod kątem zgodności z RODO, szkoli personel w zakresie ochrony danych, prowadzi rejestry wymagane przez RODO (np. rejestr czynności przetwarzania, rejestr naruszeń), a także jest punktem kontaktowym dla osób, których dane dotyczą oraz dla UODO. W kontekście bezpieczeństwa informacji IOD ściśle współpracuje z administratorem technicznym – w razie incydentów naruszenia danych doradza co do obowiązków zgłoszeniowych i metod minimalizacji ryzyka. IOD, choć nie ma kompetencji do samodzielnego wdrażania technicznych środków, sygnalizuje potrzeby i ryzyka – jego niezależność gwarantuje, że ewentualne zaniedbania zostaną zgłoszone Dyrekcji do podjęcia działań naprawczych. IOD uczestniczy w planowaniu zmian systemów informatycznych (privacy by design), opiniuje umowy powierzenia z punktu widzenia ochrony danych, jak również służy pracownikom radą w razie wątpliwości co do właściwego postępowania z danymi osobowymi.
- **Administrator Systemów Informatycznych (ASI)** – osoba (lub zespół) odpowiedzialna za techniczne zarządzanie infrastrukturą IT Muzeum. Rola ta obejmuje utrzymanie sprzętu i oprogramowania, zarządzanie kontami i uprawnieniami użytkowników, nadzorowanie bezpieczeństwa sieci, wdrażanie

aktualizacji, monitorowanie działania systemów, wykonywanie kopii zapasowych oraz pierwszą reakcję na incydenty techniczne. ASI odpowiada za implementację wielu środków opisanych w niniejszej Polityce: konfiguruje firewall i antywirusy, egzekwuje polityki haseł na systemach, zabezpiecza serwery i stacje robocze, prowadzi rejestr użytkowników i logi systemowe. W razie braku etatowego informatyka, Muzeum może powierzyć te obowiązki zewnętrznemu specjaliście lub firmie – jednak również w takim przypadku musi być jasno określone, kto pełni funkcję ASI i jakie ma obowiązki. Administrator Systemów raportuje bezpośrednio Dyrektorowi (lub wyznaczonemu Kierownikowi administracyjnemu) i współpracuje z IOD w obszarach styku techniki i ochrony danych.

- **Pracownicy Muzeum (użytkownicy systemów):** Każdy pracownik przetwarzający informacje lub korzystający z systemów IT Muzeum jest odpowiedzialny za przestrzeganie zasad niniejszej Polityki. Do ich obowiązków należy m.in. dbałość o hasła i ich poufność, właściwe zabezpieczanie stanowiska pracy, stosowanie się do klasyfikacji informacji (np. nieudostępnianie danych poufnych osobom nieuprawnionym), zgłaszanie incydentów i słabych punktów, uczestnictwo w szkoleniach z zakresu bezpieczeństwa. Pracownicy są świadomi, że bezpieczeństwo informacji jest integralną częścią ich pracy – właścicielem zasobów informacyjnych może być Muzeum, ale odpowiedzialność za ich ochronę na pierwszej linii spoczywa na nich samychgoklipka.pl. Każdy pracownik podpisuje oświadczenie o zachowaniu poufności informacji uzyskanych w trakcie pracy (obejmujące także okres po ustaniu zatrudnienia). Wszelkie naruszenia lub obawy związane z bezpieczeństwem powinni konsultować ze swoim przełożonym, IOD lub ASI – lepiej zgłosić drobną sprawę niepotrzebnie, niż przeoczyć poważne zagrożenie.
- **Kierownicy komórek organizacyjnych:** Osoby zarządzające poszczególnymi działami Muzeum (np. Dział Zbiorów, Dział Edukacji, Dział Administracyjny) mają dodatkową odpowiedzialność za zapewnienie, że podległy personel przestrzega zasad bezpieczeństwa. W ramach swoich zespołów wprowadzają dobre praktyki (np. kontrolują, czy dokumenty papierowe są właściwie przechowywane, czy stanowiska pracy są zabezpieczane). W przypadku angażowania wolontariuszy, praktykantów czy innych osób w prace działów – kierownicy dbają, by przeszły one odpowiednie szkolenie i podpisały zobowiązania do ochrony informacji.
- **Inne role specjalne:** W Muzeum mogą być ustanowione dodatkowe funkcje wspierające system bezpieczeństwa informacji, np. *Pełnomocnik ds. bezpieczeństwa informacji* (często jest to rola łączona z ASI lub IOD), odpowiedzialny za utrzymanie i doskonalenie systemu zarządzania bezpieczeństwem informacji (SZBI) jako całości; *Administratorzy poszczególnych systemów* (jeśli Muzeum używa specyficznych aplikacji, np. systemu do

ewidencji zbiorów – może być wyznaczony tzw. opiekun merytoryczny systemu, znający jego działanie i pilnujący poprawności danych, choć technicznie administracją zajmuje się ASI). Każde takie stanowisko i odpowiedzialność powinno być zdefiniowane w dokumentacji wewnętrznej (regulaminy, zakresy czynności).

Wszystkie powyższe osoby i role współpracują ze sobą dla osiągnięcia wspólnego celu, jakim jest bezpieczeństwo informacji w Muzeum. Polityka bezpieczeństwa informacji jest dokumentem żywym – będzie okresowo przeglądana (np. raz do roku lub w razie istotnych zmian prawnych/technicznych) przez powołane osoby (Dyrektora, IOD, ASI), a wszelkie aktualizacje będą komunikowane pracownikom do niezwłocznego wdrożenia. Dzięki jasno określonym obowiązkom i świadomości roli każdego pracownika, Muzeum Miejskie w Jastrzębiu-Zdroju utrzymuje wysoki poziom ochrony informacji, chroniąc zarówno bezcenne dziedzictwo kulturowe, jak i prywatność oraz zaufanie osób, z którymi współpracuje.

Źródła: Polityka opracowana na podstawie wymogów RODO (art. 24 ust. 2, art. 32) oraz wytycznych UODO, z uwzględnieniem dobrych praktyk w instytucjach kultury. W treści odwołano się m.in. do:

- przykładowych polityk bezpieczeństwa informacji w instytucjach kultury i zalecanych elementów dokumentacji ochrony danych directgroup.com.pl; dataone.pl,
- analiz specyfiki bezpieczeństwa IT muzeów, w tym zagrożeń (brak aktualizacji, brak backupów, ataki ransomware) oraz rekomendowanych rozwiązań; dataone.pl,
- decyzji i komunikatów UODO podkreślających obowiązek zawierania umów powierzenia i weryfikacji procesorów prawo.pl,
- materiałów eksperckich dot. szkoleń cybersecurity, które wskazują na krytyczne znaczenie świadomości pracowników. Wszystkie te źródła potwierdzają zasadność i kierunek przyjętych w Polityce rozwiązań. Dzięki temu dokument jest zgodny z przepisami oraz dostosowany do specyfiki Muzeum jako publicznej instytucji kultury. politykabezpieczenstwa.pl