Regulamin Bezpieczeństwa Informacji Miejskiego Zespołu Żłobków w Lublinie

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja:

1. Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin,
2. Inspektor Ochrony Danych Urzędu Miasta Lublin,

Zakres dostępu do dokumentu – odczyt:

1. Administrator - Kierownik Jednostki Organizacyjnej Gminy Lublin lub Jednostka Organizacyjna Gminy Lublin reprezentowana przez Kierownika Jednostki,
2. Pracownicy Biura Bezpieczeństwa Informacji Urzędu Miasta Lublin,
3. Kierownictwo Miejskiego Zespołu Żłobków w Lublinie,
4. Inspektor ochrony danych osobowych Miejskiego Zespołu Żłobków w Lublinie,
5. Pracownicy Miejskiego Zespołu Żłobków w Lublinie ,
6. Administratorzy Systemów Informatycznych Miejskiego Zespołu Żłobków w Lublinie ,
7. Podmioty trzecie zarządzające systemem informatycznym Miejskiego Zespołu Żłobków w Lublinie, upoważnione przez Kierownictwo Miejskiego Zespołu Żłobków w Lublinie w zakresie adekwatnym do realizowanych przez nie zadań,
8. Podmioty trzecie, które mają dostęp do danych osobowych zgromadzonych w Miejskim Zespole Żłobków w Lublinie na mocy zawartych umów w zakresie adekwatnym do realizowanych przez nie zadań.
9. Podmioty i instytucje upoważnione na podstawie przepisów prawa.

Spis treści

1 Cel

Celem dokumentu w Miejskim Zespole Żłobków w Lublinie jest:

1. określenie zasad bezpieczeństwa przy przetwarzaniu danych osobowych zarówno w formie tradycyjnej (papierowej), jak i elektronicznej,
2. zdefiniowanie zasad bezpieczeństwa informacji podczas pracy w systemach informatycznych wykorzystywanych przez Miejski Zespół Żłobków w Lublinie,
3. określenie obowiązków pracownika w zakresie przetwarzania danych i informacji chronionych.

2 Zakres

Niniejszy dokument stosują:

1. wszystkie komórki organizacyjne Miejskiego Zespołu Żłobków w Lublinie oraz wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, a także stażyści, praktykanci, wolontariusze, jak również pracownicy i współpracownicy podmiotów trzecich, z którymi zawarto umowy na mocy, których osoby te mają dostęp do danych osobowych zgromadzonych w Miejskim Zespole Żłobków w Lublinie i osoby, z którymi zawarto umowę cywilnoprawną,
2. osoby wymienione w punkcie powyżej zwane są dalej „użytkownikami".

   Dokument ma zastosowanie do informacji chronionych niezależnie od formy, w jakiej są przetwarzane i przechowywane (papierowej, elektronicznej i innej).

3 Terminologia

1. Określenia używane w dalszej treści Polityki Bezpieczeństwa Informacji i pozostałej Dokumentacji:
   a. **ADO/Administrator** – Administrator Danych Osobowych – to podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; w zależności od tego, w jakiej sytuacji są przetwarzane dane - Administratorem danych jest:
      Miejski Zespół Żłobków w Lublinie 20-411 Lublin ul. Wolska 5 reprezentowana przez Dyrektora Miejskiego Zespołu Żłobków w Lublinie zwanym dalej MZZ Lublin,
   b. **ADO UML/Administrator UML**– Administrator Danych Osobowych – Funkcję ADO pełni Prezydent Miasta Lublin,
   c. **ASI** – Administrator Systemu Informatycznego Miejskiego Zespołu Żłobków w Lublinie jest pracownik Miejskiego Zespołu Żłobków w Lublinie,
   d. **BI UML –** Biuro Bezpieczeństwa Informacji Urzędu Miasta Lublin,
   e. **CPD** – Centrum Przetwarzania Danych Urzędu Miasta Lublin,
   f. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną,

kulturową lub społeczną tożsamość osoby fizycznej. Dane osobowe dzieli się na dane zwykłe i dane szczególnej kategorii.

Jako przykład danych zwykłych można wskazać:

- numery identyfikacyjne: imię, nazwisko, adres zamieszkania, PESEL, NIP, paszport, dowód osobisty,
- cechy fizyczne: wygląd zewnętrzny, siatkówka oka, linie papilarne,
- cechy fizjologiczne: grupa krwi,
- cechy ekonomiczne: status majątkowy, lista zaległości finansowych.
- środki komunikacji elektronicznej: numer telefonu, adres e-mai.

Do danych szczególnej kategorii zaliczają się dane ujawniające:

- pochodzenie rasowe i etniczne,
- przekonania religijne czy światopoglądowe,
- przynależność do związków zawodowych czy partii,
- poglądy polityczne,
- stan zdrowia,
- kod genetyczny,
- dane biometryczne
- dane o seksualności lub orientacji seksualnej,
- wyroków skazujących i naruszeń prawa.

g. **Dostępność danych** - rozumie się przez to właściwość zapewniającą, że dane są udostępniane dla upoważnionego podmiotu wtedy, gdy ich potrzebuje do przetwarzania,

h. **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

i. **IOD – Inspektor Ochrony Danych Jednostki Organizacyjnej Gminy Lublin.**

j. **IOD UML** – Inspektor Ochrony Danych Urzędu Miasta Lublin,

k. **Jednostka/Jednostka Organizacyjna** – Miejski Zespół Żłobków w Lublinie,

l. **KJO** – Dyrektor Miejskiego Zespołu Żłobków w Lublinie,

m. **KK** – Komórka Miejskiego Zespołu Żłobków w Lublinie,

n. **KKO** – Kierownik Komórki Organizacyjnej Miejskiego Zespołu Żłobków w Lublinie,

o. **Kierownictwo Jednostki** – najwyższe kierownictwo Miejskiego Zespołu Żłobków w Lublinie,

p. **Naruszenie bezpieczeństwa informacji** – wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, obniżenia wymaganego poziomu poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur

postępowania, nawet jeżeli nie prowadzą do negatywnych skutków dla organizacji. Zdarzenia lub działania, które mogą prowadzić do naruszenia praw lub wolności osób fizycznych.

q. **Naruszenie ochrony danych osobowych** - 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,

r. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem powszechnie obowiązującym, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych, mającymi zastosowanie stosownie do celów przetwarzania. Przy czym przez sformułowanie „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe,

s. **Osoba upoważniona do przetwarzania danych osobowych** – osoba, która złożyła ADO oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,

t. **PML** – Prezydent Miasta Lublin,

u. **PSZBI** – Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin – Sekretarz Miasta, **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,

v. **Przetwarzanie** - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

w. **Poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

x. **RBI** – Regulamin Bezpieczeństwa Informacji Miejskiego Zespołu Żłobków w Lublinie,

y. **RBT UML** – Referat Bezpieczeństwa Teleinformatycznego w Biurze Bezpieczeństwa Informacji Urzędu Miasta Lublin,

z. **Regulamin/RSI** – Regulamin Systemu Informatycznego Miejskiego Zespołu Żłobków w Lublinie,

aa. **Rozliczalność danych** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

bb. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

cc. **System CPD** – system informatyczny administrowany przez Wydział Informatyki i Telekomunikacji Urzędu Miasta Lublin,

dd. **System CPD Jednostki** – system informatyczny administrowany przez Miejski Zespół Żłobków w Lublinie i zlokalizowany w CPD,

ee. **System Jednostki** – system informatyczny administrowany przez Miejski Zespół Żłobków w Lublinie i zlokalizowany w niej lub na serwerach innych niż należące do Gminy Lublin (np. serwery rządowe, serwery w chmurze obliczeniowej, i itp.).

ff. **Systemy** – System CPD, System CPD Jednostki oraz System Jednostki,

gg. **UML** – Urząd Miasta Lublin,

hh. **Usuwanie danych** – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

ii. **Usługa CPD** – usługa informatyczna administrowana przez WI,

jj. **Usługa CPD Jednostki** – usługa informatyczna administrowana przez Miejski Zespół Żłobków w Lublinie i zlokalizowana w CPD,

kk. **Usługa Jednostki** – usługa informatyczna Miejskiego Zespołu Żłobków w Lublinie administrowana przez Miejskiego Zespołu Żłobków w Lublinie i zlokalizowana w niej,

ll. **Ustawa** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000),

mm. **Uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

nn. **Użytkownik CPD** – osoba przetwarzająca dane w Systemie CPD lub Usłudze CPD, niezależnie od formy zatrudnienia lub formy prawnej wiążącej Miejski Zespół Żłobków w Lublinie z tą osobą, w szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie umowy cywilnoprawnej,

oo. **Użytkownik/pracownik (w tym podmiotu trzeciego)** - osoba przetwarzająca dane w Systemie Miejskiego Zespołu Żłobków w Lublinie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy

zatrudnienia

w Jednostce lub formy prawnej wiążącej Jednostkę z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej, wolontariusze,

pp. **WI** – Wydział Informatyki i Telekomunikacji Urzędu Miasta Lublin

qq. **Zbiór danych** – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

rr. **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.

4 Postanowienia ogólne

1. Podstawowe zasady Regulaminu Bezpieczeństwa Informacji Miejskiego Zespołu Żłobków w Lublinie, zwanym dalej RBI lub Regulaminem, określają zakres obowiązków i odpowiedzialności pracowników oraz użytkowników systemów teleinformatycznych dotyczących:
   a. bezpieczeństwa informacji przetwarzanych w formie elektronicznej oraz tradycyjnej (papierowej),
   b. przetwarzania danych osobowych,
   c. zasad postępowania w systemach teleinformatycznych.
2. Regulamin określa zasady dla poniżej wymienionych obszarów bezpieczeństwa i ochrony informacji:
   a. korzystania ze sprzętu komputerowego, systemów teleinformatycznych oraz oprogramowania,
   b. korzystania z Internetu oraz poczty elektronicznej,
   c. zabezpieczenia dostępu do danych osobowych przed dostępem osób nieuprawnionych,
   d. udostępnienia danych osobowych uprawnionym osobom,
   e. przetwarzania danych osobowych oraz innych danych podlegających ochronie w systemie informatycznym i poza systemem,
   f. zgłaszania incydentów,
   g. rozpoczęcia, wstrzymania i zakończenia pracy w systemach teleinformatycznych przez użytkowników,
   h. korzystania z urządzeń przenośnych,
   i. przechowywania dokumentów papierowych i elektronicznych oraz ich archiwizacja,
   j. fizycznych i organizacyjnych zabezpieczeń dokumentów przetwarzanych w formie tradycyjnej i elektronicznej,
   k. zasady przebywania pracowników firm zewnętrznych przebywających na terenie Miejskiego Zespołu Żłobków w Lublinie oraz nadzoru nad nimi.
3. Za zapoznanie pracowników/ użytkowników z treścią PBI, RBI oraz upoważnionych osób z RSI odpowiada Dyrektor Miejskiego Zespołu Żłobków w Lublinie lub wyznaczona przez niego osoba.

4. Potwierdzeniem zapoznania się pracowników/użytkowników z PBI oraz RSI jest złożenie podpisu na oświadczeniu stanowiącym Załącznik nr 1 do niniejszego Regulaminu.

5 Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe mogą być przetwarzane w formie tradycyjnej (papierowej) lub elektronicznej.
2. Za poprawność danych wprowadzanych do systemu informatycznego odpowiada użytkownik.
3. Dopuszcza się przetwarzanie danych osobowych w plikach arkuszy kalkulacyjnych i edytorach tekstu.
4. Dane osobowe przetwarzane w plikach mogą być kopią lub częścią bazy danych znajdującej się w systemie lub mogą być nową celową ewidencją tworzoną na potrzeby realizacji zadań związanych z przetwarzaniem danych osobowych przez uprawnione osoby.
5. Dostęp do plików z danymi powinien być ograniczony wyłącznie do osoby tworzącej taki plik na zasobach sieciowych lub na dysku lokalnym komputera. Wówczas pliki:
   a. musi być chronione hasłem, jeżeli mają być dostępne dla uprawnionych użytkowników,
   b. nie mogą być udostępnione przez sieć komputerową nieuprawnionym użytkownikom,
   c. możliwe są do otwarcia jedynie po zalogowaniu się na profil uprawnionego użytkownika.
6. W sytuacji umieszczenia plików z danymi osobowymi na serwerze plików na udziale sieciowym (tzw. dysk wspólny), dostęp do niego musi być ograniczony do określonej grupy uprawnionych użytkowników.
7. Grupę użytkowników ustala ASI lub KJO.
8. Dane osobowe znajdujące się w aplikacji pocztowej danego użytkownika, w szczególności książki adresowe, chronione są hasłem dostępowym do programu pocztowego.
9. Dane osobowe mogą być udostępniane wyłącznie za zgodą KJO, przy czym:
   a. dane osobowe udostępniać może wyłącznie ADO lub osoba przez niego upoważniona,
   b. dane osobowe można udostępniać wyłącznie na pisemny, umotywowany wniosek uprawnionych podmiotów lub osób; wniosek musi zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie,
   c. innym osobom lub podmiotom niż wymienione w pkt. b dane osobowe mogą być udostępnione, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą,
   d. udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione,
   e. ADO może odmówić udostępnienia danych, jeżeli zachodzi jakakolwiek niezgodność z RODO, czy Ustawą,
   f. Zasady powierzenia przetwarzania danych, przekazania danych i współadministrowanie danymi zostały określone w Polityce Bezpieczeństwa Informacji Miejskiego Zespołu Żłobków w Lublinie.

6 Zasady przechowywania dokumentów papierowych i elektronicznych oraz ich archiwizacja

1. Dokumenty papierowe, wydruki komputerowe:

   a. za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialni są wszyscy użytkownicy,

   b. wydruki zawierające dane osobowe przechowuje się w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych, zabezpiecza się przed dostępem osób nieupoważnionych,

   c. wszelkie wydruki zawierające inne informacje podlegające ochronie, muszą być przechowywane w miejscu niedostępnym dla osób nieupoważnionych,

   d. w przypadku, gdy do pomieszczeń po godzinach pracy mają dostęp osoby nieupoważnione, dokumenty zawierające dane osobowe zabezpiecza się na ten czas w szafach zamykanych na klucz, dotyczy to również kopii dokumentów,

   e. wydruki zawierające dane osobowe po ich wykorzystaniu lub po upływie czasu ich przydatności, należy niszczyć przy pomocy niszczarki lub przechowywać w pojemnikach przeznaczonych do bezpiecznego niszczenia dokumentacji,

   f. po zakończeniu każdego dnia pracy obowiązuje zasada „czystego biurka”,

   g. archiwizowanie papierowych zbiorów danych osobowych odbywa się w oparciu o obowiązujące w Miejskim Zespole Żłobków w Lublinie Instrukcji Kancelaryjnej, Jednolitego Rzeczowego Wykazu Akt oraz Instrukcji Archiwizacji dokumentów,

   h. klucze do szaf i biurek z dokumentami są zabezpieczane osobiście przez osoby przetwarzające.

2. Dokumenty elektroniczne - przechowywanie dokumentów:

   a. muszą być tworzone kopie zapasowe dokumentów przetwarzanych w formie elektronicznej zgodnie z zasadami określonymi przez ASI lub KJO,

   b. niestosowanie się do tych zasad (np. przechowywanie dokumentów wyłącznie na dysku lokalnym komputera) może spowodować utratę danych, za którą odpowiada użytkownik.

3. Zasady postępowania w przypadku korzystania z nośników elektronicznych (pendrive’y, zewnętrzne dyski magnetyczne, aparaty fotograficzne, dyktafony, kamery i inne):

   a. za dane przetwarzane i przechowywane na nośnikach elektronicznych odpowiada użytkownik,

b. nośniki elektroniczne zawierające dane danych osobowych, przechowuje się w szafach zamykanych na klucz, za przechowywanie tych nośników odpowiedzialni są pracownicy upoważnieni do przetwarzania danych osobowych,

c. wynoszenie na zewnątrz Miejskiego Zespołu Żłobków w Lublinie danych osobowych na nośniku elektronicznym, może odbywać się tylko za zgodą KJO,

d. informacje chronione znajdujące się na nośnikach przenośnych, wynoszonych poza teren Miejskiego Zespołu Żłobków w Lublinie, muszą być szyfrowane,

e. nośniki danych należy przechowywać w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczając je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych),

f. dane osobowe w postaci elektronicznej należy usuwać z nośnika niezwłocznie po ustaniu ich przydatności, w sposób uniemożliwiający ich ponowne odzyskanie,

g. zabrania się wyrzucania do śmieci nośników elektronicznych, w przypadku zużycia, uszkodzenia lub wymiany nośników pamięci należy bezzwłocznie je przekazać ASI lub KJO.

7 Zasady pracy w systemie teleinformatycznym oraz z dokumentacją w formie tradycyjnej

1. Rozpoczynając pracę z systemem należy sprawdzić ogólny stan używanego sprzętu oraz ocenić jakość pracy urządzenia. Należy szczególnie zwrócić uwagę na:

   a. wyświetlane niestandardowe komunikaty,

   b. automatyczne otwieranie się okienek bez związku z czynnościami wykonywanymi na komputerze,

   c. komunikaty od systemu antywirusowego.

2. Uwierzytelnienie użytkownika odbywa się zgodnie z komunikatami uruchamianego systemu. Użytkownik loguje się do systemu używając swojego identyfikatora i hasła.

3. W przypadku blokady konta systemowego, konieczność zmiany hasła lub odblokowania konta musi być zgłaszana do ASI.

4. Podczas pracy z systemie informatycznym użytkownik zobowiązany jest do stosowania podstawowych zasad bezpieczeństwa. Podczas pracy należy pamiętać w szczególności o:

   a. ustawieniu monitorów w sposób uniemożliwiający osobom nieupoważnionym na wgląd i dostęp do wyświetlanych informacji,

   b. blokowaniu dostępu do systemu operacyjnego komputera poprzez naciśnięcie przycisków Logo Windows + L lub Alt+Control+Delete potwierdzając klawiszem ENTER,

c. blokowaniu dostępu do systemu operacyjnego lub wylogowaniu się z programu przed opuszczeniem stanowiska pracy,

d. używaniu wygaszacza ekranu chronionego hasłem,

e. nadzorowaniu osób nieupoważnionych przebywających w pomieszczeniach biurowych.

5. Zabrania się w pomieszczeniach pracowniczych:

a. pozostawiania osoby nieupoważnionej bez nadzoru osoby upoważnionej,

b. zezwalania na korzystanie przez osobę nieupoważnioną z urządzeń biurowych lub sprzętu komputerowego w systemie.

6. Użytkownik jest zobowiązany do zachowania zasady czystego ekranu, tj.:

a. wylogowania się z używanego oprogramowania,

b. zamknięcia otwartych dokumentów i zapisania niezbędnych zmian,

c. zamknięcie systemu operacyjnego (należy zaczekać na jego całkowite wyłączenie).

7. Po zamknięciu systemu użytkownik sprawdza, czy nie pozostawiono bez nadzoru elektronicznych lub papierowych nośników informacji zawierających dane chronione, w szczególności dane osobowe:

a. dokumenty i nośniki elektroniczne zabezpiecza w zamykanych szafach i biurkach,

b. klucze do szaf i biurek zabezpiecza przed dostępem osób nieupoważnionych,

c. zamknąć pomieszczenia biurowe na klucz,

d. klucze do pomieszczeń zabezpiecza zgodnie z regulacjami wewnętrznymi, np. wynosi poza pomieszczenia Miejskiego Zespołu Żłobków w Lublinie, pozostawia pod nadzorem ochrony budynku.

8 Zasady haseł użytkowników

1. Hasła użytkowników do systemów muszą podlegać następującym zasadom:

a. hasło składa się z minimum 8 znaków,

b. hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#),

c. hasło musi być zmieniane minimum co 30 dni,

d. kolejne hasła muszą być różne,

e. hasła należy przechowywać w sposób gwarantujący ich poufność.

2. Zabrania się udostępniania haseł innym osobom.

3. Zabrania się tworzenia haseł na podstawie:
    a. cech i numerów osobistych (np. dat urodzenia, imion itp.),
    b. sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
    c. identyfikatora użytkownika,
4. Zabrania się tworzenia haseł łatwych do odgadnięcia.
5. Uwierzytelnienie następuje wyłącznie po podaniu prawidłowego hasła i powiązanego z nim identyfikatora.
6. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, znane tylko użytkownikowi.
7. W przypadku systemów, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego znaków, obowiązkiem użytkownika jest samodzielna cykliczna zmiana hasła zgodnie z zasadami określonymi w ust. poprzednich.
8. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
9. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i mogą być znane wyłącznie użytkownikowi.
10. Hasła nie mogą być przechowywane w formie dostępnej dla osób nieupoważnionych:
    a. w plikach,
    b. na kartkach papieru w miejscach dostępnych dla osób trzecich,
    c. w skryptach,
    d. w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
11. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, użytkownik niezwłocznie zmienia hasło lub zgłasza wniosek o zmianę hasła:
    a. do WI oraz RBT UML w przypadku hasła do Systemów CPD,
    b. do ASI lub KJO w przypadku Systemów Miejskiego Zespołu Żłobków w Lublinie.
12. Użytkownik utrzymuje hasło w tajemnicy również po upływie jego ważności.
13. Zabrania się przekazywania hasła za pomocą telefonu, przesyłania z pomocą faksu i poczty e-mail w formie jawnej (niezaszyfrowanej).
14. Uwierzytelniające karty mikroprocesorowe pozwalające zidentyfikować użytkownika na podstawie indywidualnego kodu PIN muszą być przechowywane w sposób uniemożliwiający ich zniszczenie, zagubienie lub kradzież
    (np. w zamkniętych szafkach).

15. Zabrania się udostępniania innym osobom indywidualnych identyfikatorów, w tym w szczególności loginu, tokenu, karty inteligentnej i innych danych umożliwiających uwierzytelnienie, w tym haseł, pinów, kodów i itp.

9 Korzystanie z Internetu i poczty służbowej

1. Praca w sieci Internet nie może zagrażać bezpieczeństwu danych i systemów informatycznych.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie pobrane z Internetu i przez niego zainstalowane.
3. Zabrania się w szczególności:
   a. wykorzystywania sieci Internet w sposób, który mógłby narazić Miejski Zespół Żłobków w Lublinie lub Urząd Miasta Lublin na utratę dobrego imienia, np. otwieranie stron www o złej reputacji, udostępnianie chronionych informacji na portalach społecznościowych, przesyłanie pocztą elektroniczną danych osobowych szczególnej kategorii bez zabezpieczeń,
   b. udostępniania łącza internetowego dostarczonego przez Urząd Miasta Lublin lub Miejski Zespół Żłobków w Lublinie osobom nieupoważnionym ,
   c. włączania jakichkolwiek urządzeń do infrastruktury, niebędących własnością Miejskiego Zespołu Żłobków w Lublinie lub Urzędu Miasta Lublin,
   d. obciążania sieci poprzez pobieranie filmów, plików muzycznych, gier, aplikacji i plików graficznych niezwiązanych z obowiązkami pracowniczymi.
4. Korzystając z poczty elektronicznej Miejskiego Zespołu Żłobków w Lublinie należy stosować zasady w szczególności:
   a. po odebraniu wiadomości elektronicznej upewnić się, że adres nadawcy jest prawidłowy,
   b. nie otwierać załączników z poczty e-mail, której nadawcy nie znamy,
   c. nie uruchamiać linków w poczcie e-mail, przesłanych przez nieznanych lub niezaufanych nadawców,
   d. przesyłać wiadomości wyłącznie po upewnieniu się, że adres odbiorcy jest prawidłowy, np. poprzez potwierdzenie elektroniczne otrzymania wiadomości,
   e. załączniki z danymi podlegającymi ochronie, w szczególności z danymi osobowymi szczególnej kategorii, muszą być szyfrowane (np. za pomocą programu 7zip), a hasło do ich otwarcia przekazane odbiorcy w inny sposób niż poprzez wiadomość e-mail.
5. Przesyłanie danych osobowych w innym celu, niż wykonywanie obowiązków, jest zabronione.

6. Korzystanie z prywatnej poczty elektronicznej do realizacji celów służbowych jest zabronione.
7. Korzystanie ze służbowej poczty elektronicznej do celów prywatnych jest zabronione.
8. Konfigurację oprogramowania, za pomocą którego realizuje się dostęp do zasobów Internetu, wykonuje ASI.

10 Zasady korzystania ze sprzętu komputerowego.

1. Instalacja lub deinstalacja oprogramowania, wydanie lub przekonfigurowanie sprzętu jest realizowane przez ASI.
2. Sprzęt komputerowy oraz zainstalowane na nim oprogramowanie, powierzone użytkownikowi, może być wykorzystywane tylko do celów służbowych. Zabrania się wykorzystywania ww. sprzętu i oprogramowania do celów prywatnych.
3. Użytkownik musi dbać o powierzony mu sprzęt oraz chronić go przed szkodliwym wpływem warunków zewnętrznych. Nie wolno narażać sprzętu na mechaniczne uszkodzenia oraz zalanie.
4. Należy zabezpieczać sprzęt przed kradzieżą.
5. Użytkownik zobowiązany jest przestrzegać zasady czystego biurka i czystego ekranu, w szczególności zobowiązany jest do:
    a. schowania wszystkich dokumentów, nośników danych, związanych z informacjami chronionymi w miejsce niedostępne dla innych osób po zakończeniu pracy,
    b. dbania o porządek na stanowisku pracy,
    c. zablokowania komputera przed oddaleniem się od stacji roboczej, np. naciskając jednocześnie klawisze „Logo Windows” + „L” lub wylogowując się,
    d. zamknięcia wszystkich aplikacji, wylogowania się z systemów i wyłączenia komputera po zakończeniu pracy.
6. Zabrania się użytkownikom uruchamiać i instalować na sprzęcie służbowym jakiegokolwiek oprogramowania, w tym aplikacji przenośnych niewymagających instalacji (ang. portable). Instalacji wszelkiego oprogramowania dokonuje wyłącznie ASI.
7. Zabrania się użytkownikom:
    a. omijania mechanizmów kontroli (np. używania serwerów proxy),
    b. testowania wdrożonych zabezpieczeń,
    c. skanowania urządzeń sieciowych, serwerów oraz stacji roboczych pod kątem badania świadczonych usług,
    d. wyłączania programów uruchamianych automatycznie przy starcie systemu,

e. odinstalowywania programów,

f. przyłączania i użytkowania prywatnego sprzętu, w tym prywatnych nośników danych,

g. podejmowania jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją.

8. Zabrania się przechowywania na sprzęcie służbowym gier oraz plików multimedialnych, np. filmów, zdjęć, obrazów, dźwięków niezwiązanych z zadaniami służbowymi.

9. Przed użyciem zewnętrznego nośnika danych na stacji roboczej użytkownik musi każdorazowo wykonać skanowanie programem antywirusowym wszystkich danych na nośniku.

10. W przypadku wykrycia zainfekowanych danych niezależnie od źródła (np. strona internetowa, załącznik poczty elektronicznej, dane na nośniku) należy bezzwłocznie powiadomić ASI lub KJO. Nie wolno ignorować żadnych komunikatów ostrzegawczych generowanych przez program antywirusowy oraz system operacyjny. W sytuacji pojawienia się takowych powinno się zgłosić ten fakt ASI lub KJO.

11 Zasady postępowania z komputerami przenośnymi

1. Użytkownik komputera przenośnego zawierającego dane osobowe lub inne informacje chronione zobowiązany jest zachować należytą ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w Miejskim Zespole Żłobków w Lublinie.
2. Użytkownik komputera przenośnego, zawierającego dane chronione, w szczególności dane osobowe, zobowiązany jest:
   a. stosować ochronę kryptograficzną wobec danych przetwarzanych na komputerze przenośnym,
   b. zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego stosując identyfikator i hasło,
   c. nie zezwalać na używanie komputera osobom nieupoważnionym,
   d. zachować szczególną ostrożność przy podłączaniu komputera przenośnego do sieci publicznych poza budynkami i pomieszczeniami Jednostki.
3. W przypadku podłączenia komputera przenośnego do sieci Internet poza siecią Miejskiego Zespołu Żłobków w Lublinie należy zastosować firewall zainstalowany bezpośrednio na komputerze, system antywirusowy oraz system wykrywania włamań IPS/IDS.
4. Każdy użytkownik musi zachować szczególną ostrożność podczas korzystania z zasobów sieci publicznej.
5. Komputer przenośny nie może być pozostawiany w miejscu narażającym go na kradzież (np. w otwartym pomieszczeniu, w samochodzie).
6. W przypadku pozostawienia komputerów przenośnych w miejscu pracy zaleca się po zakończeniu pracy umieszczanie ich w zamkniętych na klucz szafach lub w pomieszczeniach objętych kontrolą dostępu.
7. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego użytkownik.

12 Zasady postępowania z tabletami oraz smartfonami:

1. Użytkownik urządzenia zawierającego dane chronione, zobowiązany jest:
   a. zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem Miejskiego Zespołu Żłobków w Lublinie,
   b. zabezpieczyć dostęp na poziomie systemu operacyjnego hasłem bądź PINem,
   c. zastosować ochronę kryptograficzną wobec danych przetwarzanych na urządzeniu – o ile istnieje taka możliwość techniczna,
   d. nie zezwalać na używanie urządzenia osobom nieupoważnionym,
   e. zachować szczególną ostrożność przy podłączaniu urządzenia do sieci publicznych poza obszarem Jednostki i nie korzystać z sieci niezabezpieczonych hasłem (otwartych),
   f. zachować szczególną ostrożność podczas korzystania z sieci publicznej.
2. Urządzenie nie może być pozostawiane w sposób narażający go na kradzież.
3. W przypadku pozostawienia urządzenia w miejscu pracy, po godzinach pracy, zaleca się umieścić go w zamykanej szafie.
4. Za wszelkie działania wykonywane na urządzeniu odpowiada jego formalny użytkownik.

13 Zasady zarządzania incydentami

1. Wyróżnia się dwa rodzaje incydentów:

   a. **Incydent bezpieczeństwa informacji** – wykryte naruszenie bezpieczeństwa informacji w tym naruszenie bezpieczeństwa danych osobowych.

      Naruszeniem bezpieczeństwa informacji może być wykryte naruszenie bezpieczeństwa informacji chronionych (np. dokumentów podlegające ochronie, w tym regulaminów, procedur, schematów lub standardów bezpieczeństwa).

      Naruszeniem bezpieczeństwa danych osobowych jest każde działanie prowadzące do przypadkowego lub celowego:

      - zniszczenia
      - utraty
      - zmodyfikowania
      - nieuprawnionego ujawnienia
      - nieuprawnionego dostępu

w stosunku do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Naruszenie bezpieczeństwa danych osobowych, to sytuacja, kiedy doszło do złamania zasad ochrony danych, lub do zagrożenia bezpieczeństwa danych. Samo złamanie procedur już jest naruszeniem – staje się poważniejsze, jeśli w jego wyniku doszło do naruszenia dostępności, integralności lub poufności danych osobowych.

Katalog przykładowych incydentów bezpieczeństwa informacji oraz naruszeń danych osobowych określony jest w ***Załączniku nr 2 do niniejszego Regulaminu***

b. **Incydent cyberbezpieczeństwa** – wykryte zdarzenie w systemie informacyjnym Jednostki (systemie teleinformatycznym wraz z jego danymi), które powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Jednostkę organizacyjną Gminy.

Katalog przykładowych incydentów cyberbezpieczeństwa określony jest w ***Załączniku nr 2 do niniejszego Regulaminu. Należy zaznaczyć, że wykryte zdarzenie, może być zakwalifikowane zarówno jako incydent cyberbezpieczeństwa, jak również jako incydent bezpieczeństwa informacji (w tym naruszenie danych osobowych). Wówczas należy podjąć niżej opisane postępowania równolegle.***

2. Postępowanie w przypadku wystąpienia w Jednostce incydentu bezpieczeństwa informacji.

   a. Każde naruszenie bezpieczeństwa informacji, w tym naruszenie bezpieczeństwa danych osobowych wymaga odpowiedniej reakcji, w tym w szczególności poinformowania KJO oraz IOD o jego wystąpieniu. Obowiązek w tym zakresie spoczywa na wszystkich pracownikach i osobach trzecich, które uzyskały dostęp na mocy zawartej umowy do przetwarzanych danych.

   b. Reakcja na incydent zależy od jego istotności, mierzonej skutkami i poziomem oddziaływania na Jednostkę, Gminę Lublin lub na osoby, których dane osobowe były objęte incydentem. Ocenę w tym zakresie przeprowadza KJO w porozumieniu z IOD.

   c. W przypadku naruszenia bezpieczeństwa danych osobowych, KJO bez zbędnej zwłoki, po konsultacji z IOD – nie później niż w terminie 72 godzin od wykrycia naruszenia – zgłasza je, stosownie do postanowień art. 33 RODO, organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku zgłoszenia wystąpienia naruszenia po upływie 72 godzin do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia.

   d. W przypadku gdy naruszenie danych osobowych może powodować wysokie ryzyka naruszenia praw i wolności osób fizycznych KJO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu zgodnie z postanowieniami art. 34 RODO.

   e. Ewidencja incydentów bezpieczeństwa informacji (w tym związanych z naruszeniem ochrony danych osobowych) prowadzona jest przez IOD, zgodnie ze wzorem zawartym w ***Załączniku nr 3 do niniejszego Regulaminu,*** w formie elektronicznej lub papierowej.

3. Postępowanie w przypadku wystąpienia w Jednostce incydentu cyberbezpieczeństwa.

    a. Każde wykryte zdarzenie w systemie informacyjnym Jednostki (systemie teleinformatycznym wraz z jego danymi) i sklasyfikowane przez Jednostkę jako incydent cyberbezpieczeństwa powinno zostać zgłoszone nie później niż w ciągu 24 godzin od wykrycia do Podmiotu Krajowego Systemu Cyberbezpieczeństwa, za pośrednictwem PPK Obsługi Incydentu w UML.

Szczegółowy opis procesu zgłaszania incydentów cyberbezpieczeństwa przez Miejski Zespół Żłobków w Lublinie określony jest w „Zasadach zgłaszania incydentów cyberbezpieczeństwa przez jednostki organizacyjne Gminy Lublin" ustanowionymi przez Sekretarza Miasta Lublin, będącego osobą odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa dla wszystkich jednostek organizacyjnych Gminy Lublin.

14 Zasady przebywania na terenie Miejskiego Zespołu Żłobków w Lublinie przedstawicieli podmiotów trzecich oraz nadzoru nad nimi

1. Każda praca wykonywana w systemie teleinformatycznym lub na terenie Miejskiego Zespołu Żłobków w Lublinie przez podmioty zewnętrzne musi być zgłoszona ASI lub KJO.
2. Dostęp pracowników i współpracowników podmiotów trzecich do pomieszczeń lub systemu teleinformatycznego możliwy jest wyłącznie po uzyskaniu zgody KJO lub osoby przez niego wskazanej.
3. Zabrania się dostępu do pomieszczeń lub do systemu teleinformatycznego pracownikom podmiotów zewnętrznych bez weryfikacji ich uprawnień dostępu
4. W sytuacji podejrzenia próby nieuprawnionego dostępu, należy niezwłocznie poinformować ASI, IOD oraz KJO.

15 Postanowienia końcowe

1. Za nadzór nad przestrzeganiem postanowień Regulaminu Użytkownika odpowiada KJO.
2. Naruszając RBI, pracownik Miejskiego Zespołu Żłobków w Lublinie podlega sankcjom dyscyplinarnym, które reguluje Regulamin Pracy.
3. W przypadku naruszenia RBI, wolontariuszowi, stażyście czy też praktykantowi odbiera się niezwłocznie dostęp do danych osobowych gromadzonych w zbiorach Miejskiego Zespołu Żłobków w Lublinie.
4. Naruszając RBI, pracownik i współpracownik podmiotu trzeciego naraża go na naliczenie kary umownej określonej w umowie, na mocy której ma on dostęp do danych osobowych.

16 Lista dokumentów związanych

1. Polityka Bezpieczeństwa Informacji Miejskiego Zespołu Żłobków w Lublinie

2. Regulamin Systemu Informatycznego Miejskiego Zespołu Żłobków w Lublinie.

17 Załączniki

Załącznik nr 1 – Klasyfikacja incydentów – przykłady naruszeń bezpieczeństwa informacji oraz przykładowe incydenty cyberbezpieczeństwa

Załącznik nr 2 – Wzór oświadczenia o zapoznaniu się i zobowiązaniu do stosowania zapisów Regulaminu Bezpieczeństwa Informacji w Jednostce Organizacyjnej Gminy Lublin

Załącznik nr 3 – Wzór Rejestru incydentów bezpieczeństwa, w tym naruszeń danych osobowych