Załącznik Nr 7
do zarządzenia nr 73/12/2022
Prezydenta Miasta Leszna
z dnia 30.12.2022 r.

SYSTEM OCHRONY DANYCH I ZBIORÓW

§ 1

Zgodnie z art. 10 ust. 1 pkt 4 ustawy o rachunkowości dokumentuje się system ochrony danych i ich zbiorów w Urzędzie Miasta Leszna Wydział Finansowo-Księgowy w Lesznie:

§ 2

1. Dokumentację opisującą przyjęte przez Urząd Miasta Leszna zasady rachunkowości, księgi rachunkowe, dowody księgowe, dokumenty inwentaryzacyjne i sprawozdania finansowe, zwane zbiorami, przechowuje się w należyty sposób i chroni przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnieniem, uszkodzeniem lub zniszczeniem.
2. W jednostce budżetowej Urząd Miasta Leszna pomieszczenia, w których archiwizuje się zbiory, są zabezpieczone przed pożarem, powodzią, kradzieżą oraz dostępem osób nieupoważnionych do danych zawartych w archiwizowanej dokumentacji.
3. Przed dostępem osób nieupoważnionych do pomieszczeń, w których przechowuje się zbiory chronią zastosowane zabezpieczenia tych pomieszczeń: zamki w drzwiach oraz monitoring.
4. Zbiory przechowuje się w szafach i sejfie zamkniętych na klucz.
5. Dowody księgowe i dokumenty inwentaryzacyjne przechowuje się w Urzędzie Miasta Leszna:
   a) w oryginalnej postaci,
   b) w ustalonym porządku dostosowanym do sposobu prowadzenia ksiąg rachunkowych,
   c) w sposób pozwalający na ich łatwe odszukanie.
6. Dowody księgowe gromadzone są w segregatorach oznaczonych symbolem roku, którego dotyczą oraz początkowych i końcowych numerów dowodów księgowych.
7. Dowody księgowe przekazywane do archiwum zakładowego podlegają zszyciu i opisaniu zgodnie z przepisami dotyczącymi archiwizowania. Podlegają oznaczeniu nazwą ich rodzaju oraz symbolem roku, początkowych i końcowych numerów w zbiorze.

§ 3

W Urzędzie Miasta Leszna stosuje się następujące zasady ochrony danych komputerowych:

1. Stosowanie poniższych zasad stanowi warunek zapewnienia bezpieczeństwa danym i programom komputerowym, przechowywanym na nośnikach czytelnych dla urządzeń elektronicznego przetwarzania danych zgodnie z art. 71 ustawy o rachunkowości z dnia 29 września 1994 r.

2. Wprowadzenie i stosowanie wymienionych w niniejszym dokumencie zasad ochrony systemów informatycznych ma na celu:
   a) zabezpieczenie się przed utratą danych lub ich uszkodzeniem w stopniu uniemożliwiającym dalszą pracę, które mogą nastąpić w wyniku awarii sprzętu, oprogramowania lub wprowadzenia do systemu wirusów, tzn. programów komputerowych, których działanie polega na zakłóceniu sprawnego funkcjonowania oprogramowania lub niszczeniu, uszkadzaniu danych i aplikacji;
   b) uniemożliwienie nieautoryzowanego dostępu do programów, danych i sprzętu komputerowego, w wyniku, którego może nastąpić kradzież lub dewastacja sprzętu, uszkodzenie bądź utrata danych i programów, ujawnienie lub pozyskanie danych oraz ich nieupoważnione rozpowszechnienie;
   c) zabezpieczenie się w miarę możliwości oraz zminimalizowanie strat związanych z utratą sprzętu komputerowego wraz z przechowywanymi danymi w wyniku zdarzeń losowych (kradzież, pożary);
   d) w przypadku awarii serwerów, sieci, zasilania itp. zapewnienie możliwości wykonania procedur kończenia pracy z systemem i bezkolizyjnego przejścia na prace ręczną, tradycyjną, a po usunięciu awarii umożliwienia powrotu do systemu.

3. Wprowadza się obowiązek tworzenia kopii bezpieczeństwa danych.
   a) kopie bezpieczeństwa baz danych muszą być wykonywane przy użyciu specjalnych programów na zewnętrznych nośnikach danych. Nie wolno jednak wykonywać kopii bezpieczeństwa na nośnikach danych na stałe podłączonych do sprzętu komputerowego, na którym zainstalowane są programy finansowo-księgowe.
   b) kopie bezpieczeństwa baz danych sporządza się codziennie. Pełna kopia wykonywana jest raz na tydzień, natomiast w pozostałe dni wykonywana jest kopia pełna lub przyrostowa, zawierająca zmiany w stosunku do ostatnio sporządzonej kopii bezpieczeństwa.
   c) kopie zapasowe baz danych przechowywane są przez minimum 4 tygodnie, po tym okresie zostają one nadpisane przez nową kopię bazy.
   d) wykonując obowiązek wynikający z art. 13 ust. 6 ustawy o rachunkowości, po zamknięciu roku obrotowego dokonuje się przeniesienia treści ksiąg rachunkowych na informatyczny nośnik danych, zapewniający trwałość zapisu informacji, przez okres nie krótszy od wymaganego dla przechowywania ksiąg rachunkowych.
      Wydział Finansowo-Księgowy i Wydział Podatków i Opłat sporządza niezbędne raporty, które Biuro Informatyki przenosi na informatyczny nośnik danych w dwóch egzemplarzach. Nośniki informatyczne przechowywane są w kasach pancernych w dwóch różnych miejscach.
      Obowiązek tworzenia kopii bezpieczeństwa oraz kontrolowania jakości kopii bezpieczeństwa danych (pkt. a-c) spoczywa na Biurze Informatyki, a odpowiedzialność za terminowość i rzetelność ponosi Kierownik Biura Informatyki Urzędu Miasta Leszna.
   e) Obowiązek sporządzania raportów i wydruków ksiąg spoczywa na Naczelniku Wydziału Finansowo-Księgowego, Kierowniku Referatu Dochodów Wydziału Finansowo-Księgowego, Kierowniku Referatu Wydatków Wydziału Finansowo-Księgowego, Kierowniku Referatu Windykacji Wydziału Finansowo-Księgowego, Naczelniku Wydziału Podatków i Opłat (w zakresie wykonywanych przez ich Wydziały czynności) natomiast obowiązek dokonania zapisu na trwałym nośniku informatycznym spoczywa na Kierowniku Biura Informatyki.

4. Wprowadza się obowiązek przechowywania i tworzenia kopii bezpieczeństwa wersji wykonywalnych lub wersji instalacyjnych wyżej wymienionych programów komputerowych.
   Można odstąpić od wykonywania kopii bezpieczeństwa wersji wykonywalnych lub instalacyjnych, jeśli producent oprogramowania, zgodnie z podpisaną umową, zobligowany jest do przechowywania i udostępniania wersji instalacyjnych.
   a) Kopie bezpieczeństwa muszą być wykonane przy użyciu specjalnych programów i na zewnętrznych nośnikach danych. Pełne kopie bezpieczeństwa wersji wykonywalnych wykonywane są przez informatyka raz w tygodniu, natomiast w pozostałe dni wykonywana jest kopia pełna lub przyrostowa, zawierająca zmiany w stosunku do ostatniej kopii pełnej.
   b) Kopie bezpieczeństwa wersji instalacyjnych lub wykonywalnych należy wykonać w liczbie określonej w umowie zawartej z producentem oprogramowania lub umowie licencyjnej. W przypadku braku takich zapisów należy posiadać kopię ostatniej, poprawnie działającej wersji instalacyjnej lub wersji wykonywalnej.

5. Wprowadza się obowiązek kontrolowania wszelkich stosowanych nośników danych w celu ustalenia ewentualnej obecności na nich wirusów.
   a) Na wszystkich stacjach roboczych oraz na serwerze zainstalowane jest oprogramowanie antywirusowe. Aktualizacja oprogramowania antywirusowego oraz baz wirusów odbywa się automatycznie. Aktualizacje pobierane są z serwera producenta oprogramowania bezpośrednio po udostępnieniu przez producenta uaktualnienia.
   b) Oprogramowanie antywirusowe chroni serwery oraz stacje robocze w czasie rzeczywistym. Dodatkowo raz w miesiącu przeprowadzane jest pełne skanowanie antywirusowe na wszystkich komputerach.
   c) W przypadku stosowania przenośnych nośników danych takich jak CD-ROM itp., należy dokonywać kontroli każdorazowo po włożeniu ich do stacji czytnika. Szczególną ostrożność należy zachować przy odbieraniu wiadomości poczty elektronicznej, zawierających pliki niepewnego pochodzenia.

6. Zobowiązuje się wszystkich pracowników Wydziału Finansowo- Księgowego i Wydziału Podatków i Opłat Urzędu Miasta Leszna do ochrony danych i sprzętu komputerowego przed nieautoryzowanym dostępem. Polega ona na zabezpieczeniu w sposób fizyczny i programowy.
   a) Ochrona fizyczna komputerów wraz z zamieszczonymi na nich danymi polega na przechowywaniu ich w zamykanych pomieszczeniach. Nie wolno pozostawiać niezamkniętego pomieszczenia, w chwili, gdy nie przebywa w nim żaden z użytkowników. Inne osoby mogą przebywać w pomieszczeniu tylko w obecności użytkowników i za ich zgodą.
   b) Ochrona programowa komputerów wraz z zamieszczonymi na nich danymi polega na stosowaniu indywidualnych haseł dostępu do komputera, systemu operacyjnego oraz programów Finansowo-Księgowych, używania wygaszaczy ekranu zabezpieczanych hasłem.
   c) Nie wolno wynosić lub przesyłać żadnych danych księgowych poza jednostkę bez zgody Prezydenta Miasta Leszna lub osoby upoważnionej. Przenoszenie lub przesyłanie danych dozwolone jest po ich zabezpieczeniu przed niepowołanym odczytem w sposób programowy (hasłem lub przez zastosowanie specjalnego kodowania uniemożliwiającego ich obejrzenie przez osobę niepowołaną). Jeśli to

możliwe, należy przekazywane dane dodatkowo zabezpieczyć w sposób fizyczny (zamknięcie w kasetce).

d) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
e) W przypadku awarii/uszkodzenia nośnika danych, urządzenie to nie podlega wydaniu na zewnątrz - naprawa musi odbyć się na miejscu. W przypadku gdy naprawa okaże się niemożliwa, nośnik zostaje wymieniony na nowy, przy czym uszkodzony nośnik pozostaje w Urzędzie.
   Również wydruki zawierające dane przeznaczone do usunięcia należy zniszczyć w stopniu uniemożliwiającym ich odczytanie, w urządzeniach do tego przeznaczonych.

7. Wprowadza się obowiązek zabezpieczenia danych oprogramowania i sprzętu komputerowego przed zdarzeniami losowymi.
   a) W celu zabezpieczenia przed pożarem należy przestrzegać instrukcji i zaleceń przeciwpożarowych. W szczególności trzeba pamiętać, że nie wolno zostawiać pracującego sprzętu komputerowego bez nadzoru na okres dłuższy niż 1 godzina.
   b) Obowiązuje całkowity zakaz palenia papierosów. W celu zabezpieczenia przed innymi zdarzeniami losowymi kopie bezpieczeństwa są przechowywane w ogniotrwałym sejfie, w pomieszczeniu innym od tego, w którym przechowywane i przetwarzane są dane oryginalne. Przy przenoszeniu lub przesyłaniu kopii bezpieczeństwa należy przestrzegać przepisów dotyczących ochrony przed nieautoryzowanym dostępem do danych.

8. Wprowadza się obowiązek zapobiegania awariom sprzętu komputerowego i oprogramowania oraz zabezpieczenia przed awariami zasilania.
   a) Każdy użytkownik sprzętu komputerowego zobowiązany jest do zapoznania się i przestrzegania zasad zawartych w instrukcjach obsługi sprzętu komputerowego, podręcznikach użytkownika, a zwłaszcza w Polityce w zakresie przetwarzania danych osobowych oraz Instrukcji Zarządzania Systemem Informatycznym obowiązującym w Urzędzie Miasta Leszna
   b) Sprzęt komputerowy i programy użytkowe mogą być obsługiwane wyłącznie przez osoby, które zostały w tym zakresie przeszkolone.
   c) Nie wolno instalować oprogramowania nie przeznaczonego do celów służbowych ani oprogramowania nielicencjonowanego.
   d) Wszelkie instalacje i deinstalacje programów użytkowych i narzędziowych, przeinstalowywanie systemów operacyjnych bądź ich fragmentów (np. sterowników), powinny być realizowane przez pracowników Biura Informatyki.
   e) Jakiekolwiek instalacje dokonywane samodzielnie przez nieupoważnionego do tego użytkownika są kategorycznie zabronione i należy się liczyć z możliwością wyciągnięcia konsekwencji służbowych bądź koniecznością pokrywania ewentualnych strat.
   f) Zabrania się samodzielnego instalowania, naprawiania, rozbudowywania oraz przenoszenia sprzętu komputerowego.
   g) Zabrania się dokonywania jakichkolwiek zmian w zainstalowanych programach lub ich wersjach źródłowych bez zgody producenta oprogramowania (nie dotyczy zmian, których konieczność lub potrzeba wynika z normalnej eksploatacji systemu i nie wymaga ingerencji w strukturę informatyczną oprogramowania).

9. Wszystkie serwery oraz stacje robocze wyposażone są w urządzenia podtrzymujące zasilanie (UPS), które umożliwiają bezpieczne zakończenie pracy w systemie informatycznym w sytuacji awarii zasilania.

§ 4

W jednostce budżetowej Urząd Miasta Leszna udostępnianie dowodów księgowych, ksiąg rachunkowych i innych dokumentów z zakresu rachunkowości sprawozdań finansowych i budżetowych przebiega następująco:

a) w siedzibie jednostki – po uzyskaniu zgody kierownika jednostki lub upoważnionej przez niego osoby,
b) poza siedzibą jednostki – po uzyskaniu pisemnej zgody kierownika jednostki lub uprawnionej przez niego osoby i pozostawieniu pisemnego pokwitowania zawierającego spis wydanych dokumentów.