Załącznik Nr 9
do zarządzenia Nr 79/FK/17
Burmistrza Miasta Chełmży
z dnia 3 lipca 2017 roku

OCHRONA DANYCH

§ 1. 1. Osobą odpowiedzialną za system komputerowy i jego ochronę ustala się Administratora Systemu Informatycznego. Szczegółowe zasady określa odrębne zarządzenie Burmistrza Miasta Chełmży w sprawie ustalenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Chełmży.

2. Bezpieczna informacja komputerowa to taka, która jest chroniona przed nieupoważnionym odczytem i modyfikacją (tj. polegająca na poufności i integralności) oraz która jest dostępna i wiarygodna dla uprawnionego użytkownika (tj. polegająca na dostępności i spójności).

3. System informatyczny będzie bezpieczny, jeśli spełnione są kryteria: poufności, integralności, dostępności, spójności, rozliczalności, autentyczności i niezawodności.

1) poufność informacji komputerowej polega na ochronie informacji komputerowej, ochronie danych, itp. przed nieuprawnionym dostępem;
2) integralność to odporność informacji na nieuprawnioną modyfikację; to potrzeba zapewnienia modyfikacji danych i oprogramowania tylko w autoryzowany sposób oraz wymóg aby system realizował własne funkcje w sposób bezbłędny, niepodatny na wpływ nieautoryzowanej manipulacji systemem;
3) dostępność polega na nieograniczonej możliwości korzystania przez uprawnionych użytkowników;
4) spójność oznacza konieczność spełnienia przez system komputerowy warunków określających zależności strukturalne jej składowych;
5) kryterium rozliczalności to określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu;
6) kryterium autentyczności to możliwość weryfikacji tożsamości podmiotów lub prawdziwości aktywów systemu;
7) kryterium niezawodności to gwarancja odpowiedniego zachowania się systemu i otrzymanych wyników.

4. Należy chronić wszelkie zasoby, takie jak: oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne, występujące w systemie informatycznym lub działalności informatycznej.

5. Do najważniejszych zagrożeń należą:

1) przechwycenie informacji – naruszenie poufności;
2) modyfikacja informacji – naruszenie integralności;
3) zniszczenie informacji – naruszenie dostępności;
4) blokowanie dostępu do informacji – naruszenie dostępności.

6. Klasyfikacja powyższych zagrożeń:

1) ze względu na źródło zagrożenia:
   a) wewnętrzne,
   b) zewnętrzne,
2) ze względu na celowość działań na:
   a) przypadkowe,
   b) celowe,
3) ze względu na rodzaj zagrożenia na:
   a) programowe,
   b) sprzętowe.

§ 2. 1. Do użytkowania komputerów będących w zasobach Urzędu Miasta Chełmży dopuszczone są wyłącznie osoby w nim zatrudnione. Pomieszczenia, w których znajdują się urządzenia wchodzące w skład systemu informatycznego po zakończeniu pracy są zabezpieczane przez pracowników przed dostępem osób postronnych. Urząd posiada okablowanie strukturalne, a także odrębne pomieszczenie, w którym umieszczony jest serwer.

2. Aby programy zabezpieczyć przed dostępem osób niepowołanych, każdemu pracownikowi Wydziału Finansowo-Księgowego nadano login, hasło i uprawnienia zgodne z wykonywanymi obowiązkami. Hasło nie powinno być zbyt proste: najlepiej niech zawiera osiem i więcej znaków, jednocześnie małe i wielkie litery, liczby, znaki i żeby nie można było go znaleźć w słowniku. Hasło to jest zmieniane raz w miesiącu.

3. Nazwiska pracowników, ich hasła oraz uprawnienia są programowo zakodowane i niedostępne do odczytu.

4. Hasła mogą być również stosowane na niższych poziomach – opatrzone hasłem mogą być pojedyncze pliki zawierające dane, takie jak arkusze kalkulacyjne z planami finansowymi czy bazy z danymi osobowymi.

5. By hasło mogło być skuteczne, **musi być tajne – nie można ich nikomu podawać czy zapisywać w łatwych do znalezienia miejscach**.

6. W sieciach komputerowych dane zabezpieczane są również przez prawa dostępu, pozwalające na dostęp do określonych części sieci tylko niektórym grupom użytkowników.

7. Przed wirusami chronią programy antywirusowe, które są aktualizowane automatycznie.

8. Mechanizmy zabezpieczające przed atakami to działania służące do wykrywania, zapobiegania i likwidowania skutków ataku. Możemy rozróżnić następujące mechanizmy zabezpieczające:

1) szyfrowanie wiadomości (kryptografia);
2) uwierzytelnianie informacji (podpisy cyfrowe);
3) ochrona antywirusowa (oprogramowanie antywirusowe);
4) identyfikacja i uwierzytelnianie osób uprawnionych (hasła i loginy).

§ 3. 1. W Urzędzie zabronione jest instalowanie i używanie nielegalnych kopii programów komputerowych. Użytkownicy komputerów nie mogą samodzielnie wykonywać zmian w konfiguracji komputerów, zmiany te wykonuje wyłącznie informatyk.

2. Wszystkie dane znajdujące się w systemie informatycznym są własnością Urzędu, a ich zawartość jest objęta tajemnicą służbową. Dane zgromadzone na serwerach są archiwizowane na nośnikach komputerowych i przechowywane u Administratora.

§ 4. Ochrona danych zgromadzonych na serwerach:

1) przed dostępem nieupoważnionych osób – realizowana jest poprzez system uprawnień identyfikujący osobę, zakres danych do których ma dostęp według indywidualnych kont użytkowników, które zakłada, aktualizuje i likwiduje informatyk na pisemną prośbę. Dostęp do swojego konta i do zasobów sieci uzyskuje się poprzez system haseł;
2) przed zanikiem napięcia – realizowana jest poprzez zasilacze awaryjne UPS-y z zastosowaniem odpowiedniego programu do bezpiecznego wyłączania serwerów, listwy przeciwprzepięciowe;
3) przed utratą danych – realizowana jest poprzez stosowanie odpornych na zagrożenia nośników danych, poprzez systematyczne tworzenie rezerwowych kopii zbiorów danych, tj. na serwer NAS oraz streamer wchodzący w skład serwera obsługującego programy księgowe o numerze ewidencyjnym 4-49-491/6/2016.

§ 5. 1. Dowody księgowe i dokumenty inwentaryzacyjne przechowuje się w siedzibie jednostki w oryginalnej postaci, w ustalonym porządku dostosowanym do sposobu prowadzenia ksiąg rachunkowych, w podziale na okresy sprawozdawcze, w sposób pozwalający na ich łatwe odszukanie. Roczne zbiory dowodów księgowych i dokumentów inwentaryzacyjnych oznacza się określeniem nazwy ich rodzaju oraz symbolem końcowych lat i końcowych numerów w zbiorze.

2. Z wyłączeniem dokumentów dotyczących przeniesienia praw majątkowych do nieruchomości, list płac, powierzenia odpowiedzialności za składniki aktywów, znaczących umów i innych ważnych dokumentów określonych przez Burmistrza Miasta, po zatwierdzeniu sprawozdania finansowego treść dowodów księgowych może być przeniesiona na nośniki danych, pozwalające zachować w trwałej postaci zawartość dowodów. Warunkiem stosowania tej metody przechowywania danych jest posiadanie urządzeń pozwalających na odtworzenie dowodów w postaci wydruku, o ile inne przepisy nie stanowią inaczej.

3. Po zatwierdzeniu sprawozdania finansowego za dany rok obrotowy księgi rachunkowe oraz sprawozdania finansowe, w tym również sprawozdanie z działalności jednostki, przechowuje się odpowiednio w sposób określony w ust. 1.

4. Zbiory roczne dowodów księgowych i dokumentów inwentaryzacyjnych należy oznaczyć nazwami ich rodzajów oraz symbolami lat i numerami w zbiorach.

5. Pozostałą dokumentację z zakresu rachunkowości należy przechowywać w jednostce, co najmniej:

1) dokumentację przyjętych zasad (polityki) rachunkowości przez 5 lat od daty upływu jej stosowania;
2) księgi rachunkowe przez 5 lat od końca roku obrotowego, którego dotyczą;
3) imienne karty wynagrodzeń i pozostałe dokumenty dotyczące wynagrodzeń i ubezpieczeń społecznych przez okres 50 lat od końca ostatniego okresu rozliczeniowego;
4) dowody księgowe wieloletnich realizacji środków trwałych w budowie, pożyczek, kredytów, umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym, karny lub podatkowym – przez 5 lat od końca roku obrotowego, w którym przedmiotowe operacje gospodarcze, transakcje lub postępowania zostały ostatecznie odpowiednio: rozliczone, spłacone, zakończone lub przedawnione;
5) dokumenty dotyczące rękojmi i reklamacji – przez rok od końca okresu objętego rękojmią lub rozliczenia reklamacji;
6) dokumenty inwentaryzacyjne – 5 lat od końca roku obrotowego, którego dotyczą;

7) dowody księgowe za dany rok obrotowy, do czasu rozliczenia pracowników, którym powierzono aktywa do sprzedaży; ze względów podatkowych należałoby przechowywać te dowody księgowe przez okres 5 lat od końca roku obrotowego, którego dotyczą;
8) pozostałe dowody księgowe i dokumenty – prze 5 lat od końca roku obrotowego, którego dotyczą.

§ 6. System ochrony dowodów księgowych i innych dokumentów w formie papierowej stanowi system zabezpieczeń fizycznych, na które składają się m.in.:

1) drzwi z zamontowanymi zamkami,
2) szafy drewniane z zamkami,
3) system alarmowy.

§ 7. Udostępnienie osobie trzeciej zbiorów lub ich części:

1) do wglądu na terenie jednostki – wymaga zgody Burmistrza Miasta lub osoby przez niego upoważnionej;
2) poza siedzibą jednostki – wymaga pisemnej zgody Burmistrza Miasta oraz pozostawienia w jednostce potwierdzonego spisu przejętych dokumentów, chyba że odrębne przepisy stanowią inaczej.