Zarządzenie Nr167/2012
Wójta Gminy Osięciny
z dnia 25 stycznia 2012r.

w sprawie : zmiany ustalenia zasad prowadzenia rachunkowości oraz planów kont dla budżetu gminy, jednostek budżetowych, gminy oraz samodzielnych jednostek organizacyjnych.

Na podstawie ustawy z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2009 r. Nr 152, poz. 1223 z późn. zm.), art. 40, ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. Nr 157, poz. 1240 z późn. zm.), rozporządzenia Ministra Finansów z dnia 5 lipca 2010 r. w sprawie szczególnych zasad rachunkowości oraz planów kont dla budżetu państwa, budżetów jednostek samorządu terytorialnego, jednostek budżetowych, samorządowych zakładów budżetowych, państwowych funduszy celowych oraz państwowych jednostek budżetowych mających siedzibę poza granicami Rzeczypospolitej Polskiej (Dz. U. Nr 128, poz. 861), rozporządzenia Ministra Finansów z dnia 25 października 2010 r. w sprawie zasad rachunkowości oraz planów kont dla organów podatkowych jednostek samorządu terytorialnego (Dz. U. Nr 208, poz. 1375 (Dz. U. Nr 142 poz. 1020), w związku z art. 97 pkt. 4 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym(tj. z 2001 r. Dz. U. Nr 142 poz. 1591 z późniejszymi zmianami) ustala się co następuje :

§ 1

Załącznik Nr 2 do zarządzenia Nr 27/2011 z dnia 9 marca 2011 r w sprawie ustalenia zasad prowadzenia rachunkowości oraz planów kont dla budżetu gminy, jednostek budżetowych, gminy oraz samodzielnych jednostek organizacyjnych , otrzymuje brzmienie zgodnie z załącznikiem Nr 1 do niniejszego zarządzenia

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY OSIĘCINY

Wójt Gminy
mgr Jerzy Zydorski

Załącznik Nr 1
do Zarządzenia Nr 167/2012
Z dnia 25.01.2012

Dokumentacja systemu przetwarzania danych przy użyciu komputera

I. Dokumentacja systemu przetwarzania danych i ochrona ich zbiorów.

Zgodnie z art. 10 ust. 1 pkt. 3 i 4 i ustawy o rachunkowości. Księgi rachunkowe prowadzone za pomocą komputera i ręcznie posiadają:

- wykazy zbiorów danych tworzących księgi rachunkowe, Opisy systemu przekazania danych z określaniem struktur i wzajemnych powiązań i funkcji,
- opisy systemów informatycznych wraz z opisem algorytmów,
- datę rozpoczęcia eksploatacji tych systemów,
- system ochrony danych i ich zbiorów.

Księgi rachunkowe prowadzi się techniką komputerową wg następującego oprogramowania :

1.System Program Płatnik wer. 8 opracowany przez firmę Prokom Software SA (przekazany przez ZUS.
2.System e-PFRON OffLine opracowany przez PFRON DRQ.
3.System Besti@ opracowany przez firmę Sputnik Software.
4. Księgowość zobowiązań opracowany przez Roman i Tadeusz Groszek.
5. Podatki_xml opracowany przez Romana i Tadeusza Groszek.
6. AUTA opracowany przez Romana i Tadeusza Groszek
7. Budżet (Księgowość budżetowa)opracowany przez Romana i Tadeusza Groszek
8. Wizja opracowany przez Romana i Tadeusza Groszek
9. Zwroty opracowany przez studio programistyczne Piotra Zielonka, ul. Folwarczna 12B 97-300 Piotrków Trybunalski,
10. Podatki opracowany przez Romana i Tadeusza Groszek
11. Podatki od osób prawnych opracowany przez Romana i Tadeusza Groszek
12. Płace opracowany przez Romana i Tadeusza Groszek

Opisy w/w systemów stanowią odrębny materiał opracowany przez autorów programów.

Główną składową całego systemu jest księga główna określana jako system (FK), finansowo - księgowy, który jest na etapie wdrożenia. Stopień rozbudowy kont zależy od potrzeb naszej jednostki.

System FK daje możliwości :

- księgowanie dokumentów obrotowych na minimum dwa miesiące jednocześnie, oczy decyduje data księgowania dokumentu,
- automatyczne rozliczanie rozrachunków wielu kontrahentów,
- utworzenie katalogu tych kontrahentów,
- możliwość zakładania automatycznych źródeł rejestracji poniesionych wydatków zgodnie z klasyfikacją,
- automatycznego rozliczania wyniku finansowego.

II. Zasady ogólne.

- Wewnątrz pomieszczenia, w którym używany jest sprzęt komputerowy posiadający chronione dane, osoby nieuprawnione do ich dostępu mogą przebywać wyłącznie w obecności osoby zatrudnionej lub upoważnionej przez administratora danej jednostki komputerowej. W przypadku nieobecności takiej osoby pomieszczenia te muszą być zamykane w sposób uniemożliwiający dostęp do nich osobom postronnym.
- Po zakończeniu pracy pomieszczenia powinny być skontrolowane przez ostatniego pracownika, który je opuszcza.
- Administrator odpowiadający za bezpieczeństwo danej jednostki komputerowej zleca informatykowi wykonanie niezbędnych czynności związanych z zapewnieniem integralności danych i ich całkowitego bezpieczeństwa.
- Administrator bezpieczeństwa informacji lub osoba upoważniona, w przypadku konieczności naprawy sprzętu i oddania go do serwisu upewnia się, że dane zapisane na tzw. dysku twardym (HDD) są odpowiednio zabezpieczone lub skasowane po wcześniejszym zrobieniu kopii zapasowej na innym nośniku. W przypadku zepsucia się innej części niż HDD, jeżeli istnieje taka możliwość należy go wyjąć (w przypadku posiadania tzw. kieszeni), lub wykręcić, oddając komputer do serwisu bez tej części.

- Komputer powinien posiadać tzw. listwę zabezpieczającą, która chroni podzespoły komputera przed spaleniem spowodowanym awarią lub zakłóceniami sieci zasilającej.

- Stanowisko komputerowe posiadające bardzo ważne dane, które są nagrane na jego stałym nośniku HDD i na bieżąco na nim przetwarzane lub posiadające dostęp do takich poprzez sieć wewnętrzną (LAN) powinno być zabezpieczone tzw. urządzeniem UPS, które chroni komputer przed utratą danych spowodowanym awarią lub zakłóceniami sieci zasilającej, poprzez podtrzymywanie energii elektrycznej z baterii które zawiera.

- Do obsługi jednostek komputerowych i urządzeń do niego podłączonych, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych lub osobę przez niego upoważnioną.

- Wszyscy użytkownicy korzystający z systemu informatycznego zobowiązani są do posługiwania się swoimi stałymi „Nazwami Użytkownika" oraz „Hasłami". W przypadku zmiany któregoś z nich zobowiązane są powiadomić Kierownika Jednostki, Administratora Bezpieczeństwa Informacji lub osobę odpowiedzialną za bezpieczeństwo tych danych.

- Użytkownicy przystępujący do pracy w systemie powinni podać swoje hasło dostępu do komputera a kończąc pracę zakończyć program i wyłączyć komputer i inne urządzenia podłączone do niego.

- Każdy Użytkownik odpowiada za posiadane na swej jednostce komputerowej dane i zobowiązany jest zabezpieczyć odpowiednio ich kopie awaryjne.

- Użytkownicy tworzą w wyznaczonym terminie kopie zapasowe danych, sprawdzając je co miesiąc, pod kątem ich dalszej przydatności. Po ustaniu ich użyteczności powinny one być bezzwłocznie usuwane.

- Przeglądy i konserwacje zbiorów danych powinny być dokonywane przez poszczególnych Użytkowników lub Informatyka.

- Uprawniony Informatyk, zatrudniony w jednostce zobowiązany jest raz w miesiącu sprawdzać obecność wirusów komputerowych przy użyciu odpowiednich programów antywirusowych.

- Przegląd i konserwacja sprzętu i systemów komputerowych dokonywane winny być okresowo przez zatrudnionego Informatyka pod nadzorem Administratora Bezpieczeństwa Informacji i w obecności użytkownika danej jednostki.

- Stanowiska dostępu do chronionych danych, powinny mieć włączoną opcję automatycznego wyłączania monitorów po upływie 5 minut czasu nie aktywności Użytkownika tzw. wygaszacz ekranu, dodatkowo zabezpieczony hasłem (innym niż hasło dostępu do jednostki komputerowej).

- Monitory powinny być tak usytuowane, aby uniemożliwić odczytanie z nich chronionych danych przez osoby nieuprawnione.

- Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania Użytkownika oraz kontroli dostępu do danych, które posiada dany system informatyczny sprawuje Administrator Bezpieczeństwa Informacji.

- Administratorem Bezpieczeństwa Informacji jest Sekretarz Gminy wyznaczony zarządzeniem Wójta Gminy .

- Każda osoba przed dopuszczeniem do pracy przy chronionych danych zaznajamiana jest z przepisami dotyczącymi ich bezpieczeństwa.

III. Księgowość prowadzona za pomocą komputera.

1. Podstawą zapisów w księgach rachunków prowadzonych za pomocą komputera są :
   - sprawdzone dowody księgowe - źródłowe i zastępcze stwierdzające dokonanie operacji gospodarczych,
   - dane do komputera wprowadza się automatycznie za pośrednictwem urządzeń łączności lub komputerowych nośników danych,
   - dane tworzone wewnątrz komputera na podstawie programu, przy wykorzystaniu informacji zawartych już w księgach.

   Dane po wprowadzeniu do ksiąg rachunkowych przy użyciu komputera należy odpowiednio chronić stosując właściwe procedury i środki chroniące przed zniszczeniem, modyfikacją lub ukryciem zapisu.

   Zapis księgowy powinien zawierać co najmniej:

   - datę operacji,
   - określenie rodzaju i numer identyfikacyjny dowodu księgowego,
   - zrozumiały tekst, skrót lub kod operacji,
   - rok i datę zapisu,
   - oznaczenie kont, których dotyczy.

Na księgi rachunkowe - prowadzone za pomocą komputera i techniką ręczną składają się :

- dziennik zawierający chronologiczny ujęcie operacji wraz z nadanym automatycznie kolejnych numerem pozycji dziennika,
- konta zawierające zapisy operacji w ujęciu systematycznym, najpierw na kontach analitycznych, dopiero sumy tych obrotów wprowadzają zapisy na kontach

syntetycznych (księgi głównej),
- zestawień obrotów i sald kont, sporządzonych na koniec każdego miesiąca zawierające :

  - symbole i nazwy kont,
  - salda poszczególnych kont na dzień otwarcia konta, obroty za miesiąc i narastające od początku roku, salda na koniec miesiąca

- Obroty zestawienia obrotów i sald wymagają comiesięcznego uzgodnienia z kontem i dziennikiem, a obroty i salda z obrotami i saldami kont.

- W praktyce komputer zapewnia automatyczne uzgodnienia.

- Każdy wydruk dziennika, konta lub zestawień obrotów i sald jest trwale opatrzony:

  - nazwą jednostki,
  - rodzajem księgi i programu przetwarzania,
  - powinien zawierać określenie roku obrotowego okresu sprawozdawczego,
  - datą sporządzenia wydruku,
  - numeracją stron z oznaczeniem pierwszej i ostatniej sumowanych narastająco.

- Kontrola ciągłości zapisów oraz przenoszenia obrotów i sald następuje automatycznie.

- W myśl art. 20 ust. 5 ustawy przy prowadzeniu ksiąg rachunkowych przy użyciu komputera za równoważne z dowodami źródłowymi uważa się również zapisy w księgach rachunkowych , wprowadzane automatycznie za pośrednictwem łączności komputerowych nośników danych lub według algorytmu (programu) na podstawie informacji zawartych już w księgach pod warunkiem spełnienia następujących wymogów:

  1. Mogą one dowolnym momencie uzyskać trwale czytelną treść
  2. Możliwe jest stwierdzenie źródła pochodzenia
  3. Stosowania procedury zapewnia sprawdzenie poprawności i kompletności danych
  4. Dane źródłowe są w miejscu ich powstawania odpowiednio chronione.

- Realność danych źródłowych pozyskiwanych w formie elektronicznej musi być potwierdzone podpisem elektronicznym.

- Stawia się wymóg dekretowania zapisów źródłowych (art. 21 ust. 1 pkt. 6 ustawy) poprzez zakwalifikowanie dowodu do ujęcia w księgach rachunkowych (deklaracja) i podpis osoby odpowiedzialnej za to wskazanie.

IV. Ochrona danych, zbiorów danych i programów.

- Zgodnie z art. 23 ust. 1 ustawy należy stosować właściwe procedury i środki chroniące przed zniszczeniem, modyfikacją lub ukryciem zapisu. Zapis art. 23 ustawy uznaje księgi rachunkowe za prowadzone bezbłędnie, jeżeli wprowadzono do nich kompletnie wszystkie dowody księgowe, zapewniono ciągłości zapisów i procedur obliczeniowych (art. 23 ust. 4 ustawy).

- Zapewnić należy również wymóg identyfikacji dowodów i sposobu ich zapisania w księgach rachunkowych, na wszystkich etapach przetwarzania danych tak, aby istniał tzw. ślad rewizyjny.

- Spełniając wymogi art. 71 ustawy o ochronie danych stosowane są następujące metody zabezpieczenia dostępu do danych i ich przetwarzania poprzez :

    1. stosowanie odpornych na zagrożenie nośników danych,
    2. właściwe zabezpieczenie zewnętrznej dostępności do programów,
    3. systematyczne tworzenie rezerwowych kopii zbiorów danych zapisanych na nośnikach komputerowych przynajmniej co 5 dni,
    4. archiwizowanie bazy danych poprzez zapewnienie trwałości zapisu informatycznego systemu rachunkowości przez czas nie krótszy niż 5 lat,
    5. zabezpieczając rezerwową kopię księgi rachunkowej na nośnikach trwałych (tj. dyskietkach 3,5 calowych) lub CD-ROM, oraz okresowy wydruk kartotek.

- Wprowadzono system hasłowych zabezpieczeń chroniący przed nieupoważnionym dostępem do bazy danych lub przed zniszczeniem znany tylko administratorom systemu i kierownikowi jednostki.

V. Zasady postępowania w przypadku naruszenia ochrony danych.

- Każda osoba zatrudniona przy przetwarzaniu chronionych danych, która stwierdzi lub podejrzewa naruszenie zabezpieczeń powinna niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji albo inną upoważnioną przez niego osobę.

- Użytkownik, który uzyskał informacje lub sam stwierdził naruszenie zabezpieczeń chronionych danych zobowiązany jest niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji albo inną upoważnioną przez niego osobę.

- Administrator Bezpieczeństwa Informacji lub inna osoba upoważniona powinna w pierwszej kolejności:

  - Zapisać wszelkie informacje związane z danym zdarzeniem, a szczególnie : dokładny czas uzyskania informacji o naruszeniu bezpieczeństwa danych i czas samodzielnego wykrycia tego faktu.
  - Na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu informatycznego na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem.
  - Przystąpić do zidentyfikowania rodzaju zdarzenia, zwłaszcza skali zniszczeń i metody dostępu do danych intruza.

- Niezwłocznie podjąć odpowiednie kroki w celu powstrzymania i ograniczenia dostępu do danych przez osoby niepowołane, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji.

- Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych w systemie.

- Administrator Bezpieczeństwa Informacji lub inna upoważniona osoba powinna sprawdzić :

  - Stan urządzeń wykorzystywanych do przetwarzania chronionych danych.
  - Zawartość zbioru chronionych danych.
  - Sposób działania programu.

- Po dokonaniu powyższych czynności Administrator Bezpieczeństwa Informacji powinien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującego identyfikację:

  - Rodzaj zaistniałego zdarzenia.
  - Metody dostępu do chronionych danych intruza.
  - Skali zniszczeń.

- Niezwłocznie należy przywrócić normalny stan działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest jej odtworzenie z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu przez intruza ta samą drogą.

- Po przywróceniu prawidłowego stanu bazy chronionych danych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

  - ⊗ Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej, należy przeprowadzić dodatkowe szkolenie z zakresu bezpieczeństwa, wszystkich osób mających dostęp do chronionych danych.

  - ⊗ Jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy znaleźć źródło jego pochodzenia i wykonać niezbędne działania w celu pozbycia się go.

  - ⊗ Jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy chronionych danych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skutecznej ochrony bazy danych.

  - ⊗ Jeżeli przyczyną zdarzenia było zaniedbanie za strony osoby zatrudnionej (Użytkownika), należy wyciągnąć konsekwencje regulowane ustawą.

  - ⊗ W przypadku kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy należy powiadomić o fakcie najbliższy komisariat policji.

  - ⊗ Jeżeli przyczyną zdarzenia był zły stan techniczny sprzętu lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo - programowe.

- Administrator Bezpieczeństwa Informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia oraz natychmiast przekazuje go administratorowi chronionych danych.

Wójt Gminy
mgr Jerzy Izydorski