

w sprawie: aktualizacji zasad (polityki) rachunkowości dla budżetu gminy i jednostki Urzędu Gminy w Małej Wsi

Na podstawie art. 10 ust. 1 pkt. 3 ustawy z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2013 r. poz. 330 z późn. zm.) oraz 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 (t.j. Dz. U. z 2013 r., poz. 289 z późn. zm.)

zarządzam, co następuje:

§ 1

W „Zakładowym Planie Kont” przyjętym Zarządzeniem Nr 08/04/2011 Wójta Gminy Mała Wieś z dnia 25.01.2011 r. (zmienianym Zarządzeniem Nr 138/56/2012 z dnia 31.08.2012 r.) wprowadza się zmiany zgodnie z zapisami niniejszego Zarządzenia:

1. W Załączniku Nr 3 „Wykaz kont syntetycznych dla budżetu jednostki gminy” dodaje się konto bilansowe 290 „Odpisy aktualizujące należności” i ustala się zasady jego funkcjonowania wg Załącznika Nr 1 do niniejszego Zarządzenia.
2. Do „Zakładowego Planu Kont” dodaje się *Załącznik Nr 5* obejmujący wykaz zbiorów danych tworzących księgi rachunkowe na informatycznych nośnikach danych z określeniem ich struktury, wzajemnych powiązań oraz ich funkcji w organizacji całości ksiąg rachunkowych wraz z opisem systemu informatycznego, zgodnie z Załącznikiem Nr 2 do niniejszego Zarządzenia.

§ 2

Wykonanie zarządzenia powierza się Skarbnikowi Gminy.

§ 3

Zarządzenie wchodzi w życie z dniem podjęcia

WÓJT
Zygmunt Wojnarowski

Wykaz kont syntetycznych dla budżetu jednostki Urzędu Gminy

Konto 290 - „Odpisy aktualizujące należności”

służy do ewidencji odpisów aktualizujących wartość należności wątpliwych.

Należności wątpliwe to takie, co do których jest prawdopodobieństwo, że nie zostaną zapłacone w terminie i w pełnej wysokości, przedwczesne byłoby uznanie ich za ściągalne.

Odpisy aktualizujące należności wykonuje się na koniec roku. Zgodnie z zasadą ostrożności odpisy aktualizujące powinny uwzględniać także te przyczyny ich dokonania, które wystąpiły po dniu bilansowym, ale zostały ujawnione do dnia sporządzenia bilansu (np. zgon kontrahenta). Dokumenty stanowiące podstawę księgowania odpisu powinny szczegółowo określać przesłanki jego dokonania. Aktualizacja nie zwalnia od działań służących ściąganiu należności. Odpisy powinny być uzasadnione opisem okoliczności uprawdopodobniających ich nieściągalność(np. charakterystyka sytuacji finansowej dłużnika oraz przyczyn powstania zaległości w zapłacie należności, ocena możliwości spłaty zaległych i bieżących należności) oraz opisem czynności podjętych dla ściągania należności.

Saldo konta 290 oznacza wartość odpisów aktualizujących należności.

WÓJT
Zygmunt Wojnarowski

Dokumentacja systemu przetwarzania danych przy użyciu komputera

Zgodnie z art. 10 ust. 1 pkt. 3 i 4 i ustawy o rachunkowości, księgi rachunkowe prowadzone za pomocą komputera posiadają wykazy zbiorów danych tworzących księgi rachunkowe; opisy systemu przetwarzania danych z określaniem struktur i wzajemnych powiązań i funkcji; opisy systemów informatycznych oraz system ochrony danych i ich zbiorów.

I. KSIĘGOWOŚĆ

PROGRAM AGEMA „FK”

Do obsługi finansowo - księgowej oraz ewidencji wykonania budżetu przeznaczony jest program FINANSE KSIĘGOWOŚĆ firmy AGEMA SYSTEMY INFORMATYCZNE Łódź, który umożliwia bieżącą kontrolę wydatków budżetowych i realizację dochodów.

Przeznaczenie programu:

1. prowadzenie ksiąg rachunkowych jednostki i organu, rejestru dochodów i wydatków, prowadzenie kont w ujęciu analitycznym i syntetycznym.
2. definiowanie i wykonywanie sprawozdań finansowych i budżetowych

PROGRAM PŁACE

Ewidencja szczegółowa dotycząca rozrachunków z tytułu wynagrodzeń z pracownikami, zleceniobiorców oraz rozrachunków publiczno-prawnych z nimi związanych odbywa się za pomocą programu płacowo-kadrowego KADRY PŁACE firmy AGEMA SYSTEMY INFORMATYCZNE Łódź.

Przeznaczenie programu:

- 1) ewidencja informacji kadrowych,
- 2) naliczanie płac, podatku od wynagrodzeń,
- 3) zasiłków chorobowych i macierzyńskich,
- 4) sporządzanie deklaracji PIT 4R, PIT 11,
- 5) przeliczenie i przygotowanie deklaracji ZUS (jako plik do eksportu do PŁATNIKA).

PROGRAM PŁATNIK

Przeznaczenie – rozliczenia z ZUS w zakresie składek na ubezpieczenie społeczne, zdrowotne i Fundusz Pracy.

PROGRAM BESTIA

program Firmy SPUTNIK SOFTWARE przeznaczony do zarządzania budżetami jednostek samorządu terytorialnego. Przeznaczenie programu:

- 1) definiowanie i wykonywanie sprawozdań finansowych/budżetowych jednostkowych i zbiorczych;
- 2) opracowywanie zmian w postaci uchwał i zarządzeń dotyczących realizacji budżetu gminy i Wieloletniej Prognozy Finansowej,
- 3) komunikacja z Regionalną Izbą Obrachunkową w Warszawie, Zespół w Płocku

HOME BANKING

System bankowości elektronicznej obsługiwany przez bank prowadzący obsługę księgową gminy służy do komputerowego sporządzania przelewów, wyciągów bankowych, potwierdzeń dokonanych przelewów oraz analizowania historii obrotów na rachunkach bankowych jednostki.

PROGRAM ŚRODKI TRWAŁE

Program Firmy SPUTNIK SOFTWARE zapewnia pełną obsługę w zakresie ewidencji środków trwałych, wyposażenia, wartości niematerialnych i prawnych oraz gruntów

PROGRAM PODATKI

system firmy SoftHard Płock, umożliwia: wymiar łącznego zobowiązania pieniężnego; tworzenie dokumentacji wymiarowej: lista podatków, lista podatników, wprowadzanie i korekta danych podatnika, naliczanie należności podatkowych.

KSIEGOWOŚĆ PODATKOWA

program firmy Usługi Informatyczne PRO-INFO Ozorków, umożliwia księgowanie wpłat, drukowanie konto kwitariuszy, rozliczenie podatku poprzez zestawienia, listy i kartoteki.

PROGRAM ODPADY KOMUNALNE

Program firmy ULISSES Sp. z o.o. z/s Kalisz obejmuje całość zagadnień wynikających ze znowelizowanej ustawy o utrzymaniu czystości i porządku w gminie, tj. karty kontowe podatników, decyzje o ustaleniu opłaty, o ustaleniu zaległości, o odroczeniu terminu, o umorzeniu, o rozłożeniu na raty, windykacja (upomnienie, odwołanie, tytuł wykonawczy, harmonogram opłat) itp.

II. Księgowość prowadzona za pomocą komputera.

Podstawą zapisów w księgach rachunków prowadzonych za pomocą komputera są sprawdzone dowody księgowe - źródłowe i zastępcze stwierdzające dokonanie operacji gospodarczych.

Jednostka posiada odpowiednie oprogramowanie umożliwiające uzyskiwanie czytelnych informacji w odniesieniu do zapisów dokonanych w księgach rachunkowych, poprzez ich przeniesienie na informatyczny nośnik danych. Treść ksiąg rachunkowych nie później niż na koniec roku obrotowego przenoszona jest na informatyczny nośnik danych, zapewniający trwałość zapisu informacji, przez czas nie krótszy od wymaganego dla przechowywania ksiąg rachunkowych.

Na księgi rachunkowe - prowadzone za pomocą komputera składają się:

- 1) dziennik zawierający chronologiczne ujęcie operacji wraz z nadanym kolejnym numerem pozycji dziennika,
- 2) konta zawierające zapisy operacji w ujęciu systematycznym, najpierw na kontach analitycznych, dopiero sumy tych obrotów wprowadzają zapisy na kontach syntetycznych (księgi głównej),
- 3) 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 narastająco 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.

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

- nazwa jednostki,
- rodzaje księgi i programu przetwarzania,
- określenie roku obrotowego okresu sprawozdawczego,
- daty sporządzenia wydruku,
- numerację 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:

- mogą one w dowolnym momencie uzyskać trwale czytelną treść,
- możliwe jest stwierdzenie źródła pochodzenia,
- stosowania procedury zapewnia sprawdzenie poprawności i kompletności danych,
- dane źródłowe są w miejscu ich powstawania odpowiednio chronione.

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

Program - System Finansowo Księgowy AGEMA „FK umożliwia zakładanie lub przenoszenie (w nowym roku obrotowym) obowiązującego planu kont poprzez wpisanie symbolu konta, jego nazwy, strony księgowania oraz następujących parametrów: czy jest to konto bez wprowadzania obrotów, czy jest ono syntetyczne oraz czy jest kontem pozabilansowym. Istnieje możliwość dopisywania kont w czasie eksploatacji programu.

Rejestracja dowodów rozpoczyna się od wskazania jakiego miesiąca mają dotyczyć zdarzenia gospodarcze określone w danym dowodzie księgowym. Data księgowania to data, według której sporządzany jest dziennik oraz odzwierciedla ona chronologię zapisów na kontach księgowych.

W dalszej części wprowadzane są następujące dane:

1. numer pozycji i numer dowodu księgowego;
2. tekst – pole służące słownemu opisowi zdarzenia gospodarczego;
3. konto Wn i kwota Wn; konto Ma i kwota Ma;
4. data zapłaty;
5. symbol dowodu budżetowego;
6. symbol klasyfikacji budżetowej,
7. symbol i klasyfikacja wydatku strukturalnego; kwota wydatku strukturalnego.

System umożliwia na bieżąco sprawdzanie bilansowania się dowodu. Proces księgowania dzienników powoduje dokonanie zapisu na kontach księgi głównej. Wszystkie zdarzenia

gospodarcze z dowodów dotyczących bieżącego okresu obliczeniowego są trwale zapisane w układzie chronologicznym. Wszelkich zmian dokonuje się za pomocą dokumentów stornujących.

Program „F-K” współpracuje z programem „Bestia” w zakresie automatycznego przekazywania sprawozdań budżetowych.

III. Ochrona danych, zbiorów danych i programów.

Mechanizmy programowe

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

1. Pod pojęciem ochrony danych rozumiane jest zabezpieczenie informacji przed dostępem do nich osób niepowołanych, a także zapewnienie możliwości ich odzyskania w przypadku awarii systemu. Dla zmniejszenia ryzyka ewentualnej utraty danych należy tworzyć kopie zapasowe systemu, stanowiące jego replikę na dysku twardym. Kopiowanie powinno odbywać się na inny dysk niż ten, na którym eksploatowany jest system. Niezmiernie istotne jest częste sporządzanie kopii, co ogranicza do minimum konieczność powtórnego wprowadzania utraconych dokumentów. Kopie baz danych tworzy się na serwerze codziennie poza godzinami pracy użytkowników. W przypadku utraty danych w programie korzysta się z funkcji odtwarzania danych z kopii. Operacja ta powinna być traktowana jako ostateczność, bowiem jej wykonanie równoznaczne jest z usunięciem z katalogu zbiorów z bieżącymi danymi.
2. W celu ochrony danych od świadomego usunięcia danych przez użytkowników stosuje się odpowiedni system haseł oraz przynależność do odpowiednich grup. Wejście do wszystkich programów chronione jest nazwą użytkownika oraz hasłem przypisanym konkretnemu użytkownikowi. W przypadku zmiany któregoś z nich zobowiązany jest powiadomić Administratora Systemu Informatycznego.

Rozwiązania techniczno - organizacyjne

1. 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.

2. W celu ochrony sprzętu komputerowego przed uszkodzeniem spowodowanym niewłaściwymi parametrami zasilania z sieci energetycznej, wymagane jest podłączenie komputerów do odpowiednio przystosowanej w tym celu instalacji elektrycznej lub też podłączanie komputerów do sieci energetycznej za pomocą tzw. UPS – zasilaczy awaryjnych. Monitory powinny być tak usytuowane, aby uniemożliwić odczytanie z nich chronionych danych przez osoby nieuprawnione.
3. Każda osoba przed dopuszczeniem do pracy przy chronionych danych zaznajamiana jest z przepisami dotyczącymi bezpieczeństwa oraz ich polityką.

IV. Zasady postępowania w przypadku naruszenia ochrony danych.

1. Każda osoba zatrudniona przy przetwarzaniu chronionych danych, która stwierdzi lub podejrzewa naruszenie zabezpieczeń powinna niezwłocznie powiadomić o tym Administratora Systemu Informatycznego.
2. Użytkownik, który uzyskał informacje lub sam stwierdził naruszenie zabezpieczeń chronionych danych zobowiązany jest niezwłocznie powiadomić o tym Administratora Systemu Informatycznego.
3. Administrator 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
 - 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,
 - 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 osobę niepowołaną tą 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 oraz ograniczyć jej uprawnienia (brak możliwości kasowania zawartości 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 był zły stan techniczny sprzętu lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo - programowe.

WÓJT
Zygmunt Wojnarowski