SYSTEM OCHRONY DANYCH W JEDNOSTCE
(załącznik nr 7)

**1.Ochrona zbiorów ksiąg rachunkowych**

Ochronę przed dostępem osób nieupoważnionych zapewniają sprawdzone zabezpieczenia pomieszczeń, w których przechowuje się zbiory księgowe. Są to zamki zamontowane w drzwiach oraz alarm przeciwwłamaniowy w budynku.

Dodatkowym zabezpieczeniem dla przechowywanych dokumentów są odpowiednie szafy.

Szczególnej ochronie poddane są:

- sprzęt komputerowy użytkowany w Referacie Finansowym ,

- księgowy system informatyczny,

- kopie zapisów księgowych,

- dowody księgowe,

- dokumentacja inwentaryzacyjna,

- sprawozdania budżetowe i finansowe,

- dokumentacja rachunkowa opisująca przyjęte przez jednostkę zasady rachunkowości.

Dla prawidłowej ochrony ksiąg rachunkowych stosuje się:

- regularne wykonywanie kopii bezpieczeństwa,

- odpowiedni poziom zarządzania dostępem do danych pracowników na różnych stanowiskach (imienne konta użytkowników z bezpiecznie przechowywanymi hasłami dostępu, możliwość różnicowania dostępu do baz danych i dokumentów w zależności od zakresu obowiązków danego pracownika),

- profilaktykę antywirusową – opracowane i przestrzegane odpowiednie procedury oraz stosowane programy zabezpieczające,

- zabezpieczenia przed atakiem z zewnątrz,

- odpowiednie systemy bezpiecznej transmisji danych,

- systemy podtrzymywania napięcia w razie awarii sieci energetycznej (UPS),

Kompletne księgi rachunkowe drukowane są nie później niż na koniec roku obrotowego. Za równoważne z wydrukiem uznaje się przeniesienie treści ksiąg rachunkowych na inny informatyczny nośnik danych, zapewniający trwałość zapisu informacji, przez czas nie krótszy niż 5 lat, licząc od początku roku następującego po roku obrotowym, którego dane zbiory dotyczą.

**2. Wydawanie uprawnień do wprowadzenia danych do systemów informatycznych:**

* uprawnienie do obsługi systemów informatycznych są wydawane na podstawie zakresu czynności pracownika,
* pracownik jest odpowiedzialny za wszystkie wykonane czynności w systemie, ich treść merytoryczną i dokonywane korekty,
* pracownik nie może wykonywać czynności, do których nie jest uprawniony,
* wszystkie czynności wykonywane przez pracownika mogą być kontrolowane przez głównego księgowego,
* w przypadku utraty uprawnień administrator sieci i systemów komputerowych niezwłocznie blokuje dostęp do systemu i informuje bezpośredniego przełożonego pracownika.

**3. Obowiązki pracownika w zakresie wykorzystywania nadanego hasła i uprawnień:**

* pracownik nie może udostępniać swojego hasła osobie nieupoważnionej,
* w przypadku podejrzenia o poznanie hasła przez osobę nieupoważnioną, należy ten fakt niezwłocznie zgłosić do administratora systemu,
* pracownik jest zobowiązany do wykorzystania programu zgodnie z jego przeznaczeniem,
* zabrania się dokonywania samodzielnie napraw przez pracownika w przypadku awarii systemu (o tym fakcie należy powiadomić administratora systemu),
* po zakończeniu pracy należy obowiązkowo wylogować się z systemu,
* kategorycznie zabrania się wyłączenia komputera bez zamknięcia systemu informatycznego i sieci.

**4. Archiwizowanie zbiorów danych i zabezpieczenie:**

* za wytworzone informacje odpowiada bezpośrednio operator systemu , a pośrednio z racji swoich obowiązków administrator systemu,
* archiwizacja jest dokonywana raz na tydzień,
* do zabezpieczenia wykorzystuje się dyski twarde i serwery oraz dyski CD, DVD.

**5. Przechowywanie danych i ochrona:**

* wszystkie elektroniczne nośniki informatyczne są przechowywane w urzędzie i nie powinny być bez decyzji kierownik jednostki wynoszone,
* nośniki informacji bezpośrednio są przechowywane w szafach lub metalowych sejfach,
* zabrania się udostępniania nośników poza siedzibę jednostki bez zgody kierownika jednostki,
* wszystkie programy i stanowiska pracy maja zainstalowane programy antywirusowe i inne zabezpieczenia,
* kategorycznie zabrania się instalowania w systemie prywatnych programów użytkowych,

**6. Procedury wykonywania przeglądów i konserwacji systemu:**

* za terminową konserwację systemu jest odpowiedzialny administrator systemu,
* administrator jest reprezentantem kierownika jednostki w kontaktach z producentem/autorem oprogramowania,
* administrator systemu prowadzi na bieżąco ewidencję dokonanych przeglądów i konserwacji

**7. Przechowywanie zbiorów**

W sposób trwały (nie krótszy niż 50 lat) przechowywane są zatwierdzone sprawo­zdania finansowe, a także dokumentacja płacowa (listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty), licząc od dnia, w którym pracownik przestał pracować u danego płatnika składek na ubezpieczenia społeczne (art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z FUS, t.j. Dz.U. z 2009 r. Nr 153, poz. 1227 z późn. zm.).

Okresowemu przechowywaniu podlegają:

- dowody księgowe dotyczące środków trwałych w budowie, pożyczek, umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym lub objętych postępowanie karnym albo podatkowym – przez okres 5 lat od początku roku następującego po roku obrotowym, w którym operacje, transakcje i postępowanie zostały ostatecznie zakończone, spłacone lub uległy przedawnieniu,

- dokumentacja przyjętego sposobu prowadzenia rachunkowości – przez okres nie krótszy niż 5 lat od upływu ich ważności,

- dokumenty dotyczące rękojmi i reklamacji – 1 rok po terminie upływu rękojmi lub rozliczeniu reklamacji,

- księgi rachunkowe, dokumenty inwentaryzacyjne oraz pozostałe dowody księgowe i dokumenty – przez okres 5 lat,

- dokumentacja związana z projektami finansowanymi ze środków Unii Europejskiej i innych państw oraz organizacji międzynarodowych jest przechowywana przez okres określony w wytycznych zawartych w dokumentach odpowiedniego programu lub instrukcjach dotyczących źródeł finansowania danego projektu albo w umowie o dofinansowanie, chyba że przepisy krajowe zakładają dłuższy okres przechowywania niektórych z nich, to dla tych dokumentów stosuje się odpowiednio przepisy krajowe.

Powyższe terminy oblicza się od początku roku następującego po roku obrotowym, którego dane zbiory (dokumenty) dotyczą.

W przypadku zakończenia działalności jednostki na skutek:

- połączenia z inną jednostką lub przekształcenia formy prawnej – zbiory będą przechowywane przez jednostkę kontynuującą działalność.

- jej likwidacji – zbiory przechowuje wyznaczona osoba lub jednostka; o miejscu przechowywania kierownik jednostki informuje właściwy organ prowadzący ewidencję działalności.

8. Udostępnianie danych i dokumentów

Udostępnienie sprawozdań finansowych i budżetowych oraz dowodów księgowych, ksiąg rachunkowych i innych dokumentów z zakresu rachunkowości jednostki ma miejsce:

- w siedzibie jednostki po uzyskaniu zgody kierownika jednostki lub upoważnionej przez niego osoby,

- poza siedzibą jednostki po uzyskaniu pisemnej zgody kierownika jednostki i pozo­stawieniu pisemnego pokwitowania zawierającego spis wydanych dokumentów.

Zbiory jednostek, które :

-zakończyły swoją działalność w wyniku połączenia z inną jednostką lub przekształcenia formy prawnej-przechowuje jednostka kontynuująca działalność,

- zostały zlikwidowane –przechowuje wyznaczona osoba lub jednostka; o miejscu przechowywania kierownik, likwidator jednostki lub syndyk masy upadłościowej informuje właściwy sąd lub inny organ prowadzący rejestr.