Zarządzenie nr 0050.24.2023
Wójta Gminy Lubanie
z dnia 18 kwietnia 2023 roku

zmieniające zarządzenie w sprawie wprowadzenia zasad (polityki) rachunkowości

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz. U. z 2022 roku poz. 559 z późn. zm), rozporządzenia Ministra Rozwoju i Finansów z dnia 3 lutego 2020 roku w sprawie 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. z 2020 roku, poz. 342) w związku z art. 16a i 16d ust. 1 ustawy z dnia 15 lutego 1992 roku o podatku dochodowym od osób prawnych (Dz. U. z 2020 roku, poz. 2587 z późn. zm.) zarządzam co następuje:

§ 1

W polityce rachunkowości dla budżetu gminy i Urzędu Gminy w Lubaniu przyjętej Zarządzeniem Wójta Gminy Lubanie nr 0050.58.2017 z dnia 15.12.2017 roku w sprawie wprowadzenia zasad (polityki) rachunkowości zmienionej zarządzeniem nr 0050.54.2019 Wójta Gminy Lubanie z dnia 16 września 2019 roku i zarządzeniem nr 0050.92A.2022 Wójta Gminy Lubanie z dnia 14 listopada 2022 roku

wprowadza się następujące zmiany:

Załącznik nr 4 Dokumentacja systemu ochrony i przetwarzania danych przy użyciu komputera otrzymuje brzmienie:

I. Dokumentacja systemu przetwarzania danych i ochrona ich zbiorów.

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

- wykazy zbiorów danych tworzących księgi rachunkowe, opisy systemu przekazania danych z określeniem 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:

- PŁACE – Tadeusza i Romana Groszka,
- PODATKI i KSIĘGOWOŚĆ - Tadeusza i Romana Groszka,
- INFO – SYSTEM - Tadeusza i Romana Groszka,

- LEX – Wolters Kluwer Polska S.A.,
- BUDŻET ST - Tadeusza i Romana Groszka,
- Środki Trwałe

II. Zasady ogólne.

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.
2. Po zakończeniu pracy pomieszczenia powinny być skontrolowane przez ostatniego pracownika, który je opuszcza.
3. Pomieszczenia, w których znajdują się stanowiska komputerowe muszą być okratowane od strony okien.
4. Administrator odpowiadający za bezpieczeństwo danej jednostki komputerowej zleca informatykowi wykonanie niezbędnych czynności związanych z zapewnieniem integralności danych i ich całkowitego bezpieczeństwa.
5. 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.
6. 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.

7. 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.
8. 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.
9. Użytkownicy przystępujący do pracy w systemie powinni posiadać swoje hasło dostępu do komputera a kończąc pracę zakończyć program i wyłączyć komputer oraz inne urządzenia podłączone do niego.
10. Każdy Użytkownik odpowiada za posiadane na swojej jednostce komputerowej dane i zobowiązany jest zabezpieczyć odpowiednio ich kopie awaryjne.
11. 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.
12. Przeglądy i konserwacje zbiorów danych powinny być dokonywane przez poszczególnych Użytkowników lub Informatyka.
13. Uprawniony Informatyk, zatrudniony w jednostce zobowiązany jest raz w miesiącu sprawdzać obecność wirusów komputerowych przy użyciu odpowiednich programów antywirusowych.
14. Przegląd i konserwacja sprzętu i systemów komputerowych dokonywane winny być okresowo przez zatrudnionego Informatyka pod nadzorem Administratora Bezpieczeństwa Informacji w obecności użytkownika danej jednostki.
15. 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).
16. Monitory powinny być tak usytuowane, aby uniemożliwić odczytanie z nich chronionych danych przez osoby nieuprawnione.
17. Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania Użytkownika oraz kontroli dostępu do danych, które posiada dany system informatyczny sprawuje Administrator Bezpieczeństwa Informacji.

18. Administratorem Bezpieczeństwa Informacji jest Sekretarz Gminy Lubanie wyznaczony zarządzeniem Wójta Gminy Lubanie.
19. 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.
2. 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.
3. Na księgi rachunkowe – prowadzone za pomocą komputera i techniką ręczną składają się:
   - dziennik zawierający chronologiczne 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),
   - zestawienia obrotów i sald kont, sporządzane 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

4. Obroty, zestawienia obrotów i sald wymagają comiesięcznego uzgodnienia z kontem i dziennikiem, a obroty i salda z obrotami i saldami kont.
5. W praktyce komputer zapewnia automatyczne uzgodnienia.
6. 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.
7. Kontrola ciągłości zapisów oraz przenoszenia obrotów i sald następuje automatycznie.
8. 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, wprowadzone 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,
   - stosowanie procedury zapewnia sprawdzenie poprawności i kompletności danych,
   - dane źródłowe są w miejscu ich powstania odpowiednio chronione.
9. Realność danych źródłowych pozyskiwanych w formie elektronicznej musi być potwierdzona podpisem elektronicznym.
10. Stawia się wymóg dekretowania zapisów źródłowych (art. 21 ust. 1 pkt. 6 ustawy) poprzez zakwalifikowane dowodu do ujęcia w księgach rachunkowych (deklaracja) i podpis osoby odpowiedzialnej za to wskazanie.

IV. Ochrona danych, zbiorów danych i programów.

1. Zgodnie z art. 23 ust. 1 ustawy należy stosować właściwe procedury i środki chroniące przed zniszczeniem, modyfikacja lub ukryciem zapisu. Zapis art. 23

ustawy uznaje księgi rachunkowe za prowadzone bezbłędnie, jeżeli wprowadzono do nich kompletnie wszystkie dowody księgowe, zapewniono ciągłość zapisów i procedur obliczeniowych (art. 23 ust. 4 ustawy).

2. Zapewnić należy również wymóg identyfikacji dowodów i sposobu ich zapisania w księgach rachunkowych, na wszystkich etapach przetwarzania danych tak, aby istniał tzw. ślad rewizyjny.
3. Spełniając wymogi art. 71 ustawy o ochronie danych stosowane są następujące metody zabezpieczenia dostępu do danych i ich przetwarzania poprzez:
   - stosowanie odpornych na zagrożenie nośników danych,
   - właściwe zabezpieczenie zewnętrznej dostępności do programów,
   - systematyczne tworzenie rezerwowych kopii zbiorów danych zapisanych na nośnikach komputerowych przynajmniej, co 5 dni,
   - archiwizowanie bazy danych poprzez zapewnienie trwałości zapisu informatycznego systemu rachunkowości przez czas nie krótszy niż 5 lat,
   - wszystkie dane z komputerów pracowników są kopiowane na zewnętrzny dysk sieciowy znajdujący się w innym pomieszczeniu niż serwer, dodatkowa kopie są przechowywane w chmurze (na serwerze poza siedzibą firmy)
4. 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.

1. 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.
2. Użytkownik, który uzyskał informację lub sam stwierdził naruszenie zabezpieczeń chronionych danych zobowiązany jest niezwłocznie powiadomić o tym Administratora Bezpieczeństwa informacji albo inną upoważnioną przez niego osobę.
3. 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.

4. Niezwłocznie podjąć odpowiednie kroki w celu powstrzymania i ograniczenia dostępu do danych przez osoby niepowołane, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji.
5. Po wyeliminowaniu bezpośrednio zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych w systemie.
6. Administrator bezpieczeństwa informacji lub inna upoważniona osoba powinna sprawdzić:
   - stan urządzeń wykorzystywanych do przetwarzania chronionych danych,
   - zawartość zbioru chronionych danych,
   - sposób działania programu.
7. Po dokonaniu powyższych czynności Administrator Bezpieczeństwa informacji powinien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującego identyfikacją:
   - rodzaj zaistniałego zdarzenia,
   - metody dostępu do chronionych danych intruza,
   - skali zniszczeń.
8. 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 tą samą drogą.
9. 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,
- 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.

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

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia i podlega publikacji w Biuletynie Informacji Publicznej.

WÓJT GMINY
mgr Lacysa Krzyżańska