Centrum Usług Wspólnych

Centrum Usług Wspólnych w Białogardzie
ul. 1 Maja 18, 78-200 Białogard
tel.: 94 3579 350
cuw@bialogard.info
http://bip.cuw.bialogard.info

Zarządzenie nr 26/IV/2022

Dyrektora Centrum Usług Wspólnych w Białogardzie

z dnia 04.04.2022 roku

zmieniające zarządzenie w sprawie ustalenia dokumentacji przyjętych zasad (polityki) rachunkowości w Centrum Usług Wspólnych w Białogardzie

Na podstawie:

1/ art. 40 ustawy o finansach publicznych z dnia 27 sierpnia 2009 r. (tj. Dz. U. 2021 r. poz. 217, z późn. zm.),

2/ art. 10 i 13 ustawy o rachunkowości z dnia 29 września 1994 r. (tj. Dz. U. z 2021 r., poz. 305, z późn. zm.),

3/ § 15 rozporządzenia Ministra Rozwoju i Finansów z dnia 13 września 2017 r. 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 (tj. Dz. U. z 2020 r. poz. 342, z późn. zm.) zarządza się, co następuje:

§ 1. W zarządzeniu nr 10/2020 Dyrektora Centrum Usług Wspólnych w Białogardzie z dnia 30 listopada 2020 r. w sprawie ustalenia dokumentacji przyjętych zasad (polityki) rachunkowości w Centrum Usług Wspólnych w Białogardzie Rozdział 5 System służący ochronie danych i zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów otrzymuje brzmienie określone w załączniku do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podjęcia.

Załącznik do Z. 26/IV/2022
z dnia 4 kwietnia 2022 r.
Dyrektora CUW w Białogardzie

Rozdział 5 System służący ochronie danych i zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów

1. Ochrona zbiorów ksiąg rachunkowych

1. System ochrony danych rozpatrywany jest w trzech aspektach:
   1. stworzono odpowiednie warunki techniczno-organizacyjne eksploatacji systemu,
   2. mechanizmów programowych,
   3. oraz archiwizowania i przechowywania danych.
2. Zabezpieczono pomieszczenia (wprowadzono ochronę przeciwpożarową, ograniczono dostęp do pomieszczeń), starannie dobrano sprzęt, zastosowano urządzenia zapewniające niezakłóconą pracę komputerów (zainstalowano bezprzerwowe zasilacze awaryjne (UPS).
3. Ochronę przed dostępem osób nieupoważnionych zapewniają sprawdzone zabezpieczenia pomieszczeń CUW, w których przechowuje się zbiory księgowe. Są to atestowane zamki zamontowane w drzwiach oraz zabezpieczenia w postaci monitoringu. Pomieszczenia zamykane są przez pracowników CUW. Po zakończeniu pracy pomieszczenia są kontrolowane przez ostatniego pracownika, który je opuszcza. Po godzinach pracy w pomieszczeniach przebywa tylko osoba sprzątająca.
4. Dodatkowym zabezpieczeniem dla przechowywanych dokumentów są odpowiednie szafy.
5. Szczególnej ochronie poddane są:
   1. sprzęt komputerowy użytkowany w dziale księgowości,
   2. kopie zapisów księgowych,
   3. dowody księgowe,
   4. dokumentacja inwentaryzacyjna,
   5. sprawozdania budżetowe i finansowe,
   6. dokumentacja rachunkowa opisująca przyjęte przez jednostkę zasady rachunkowości.
6. Zapisy w księgach rachunkowych dokonywane są w sposób zapewniający ich trwałość, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych.

7. Program Progman Finanse DDJ ogranicza dostęp do danych między innymi poprzez konieczność podania hasła w momencie uruchamiania systemu. Hasło to jest przypisane konkretnemu użytkownikowi. Podczas wpisywania nie pojawia się ono na ekranie. Ma to na celu zabezpieczenie przed podpatrzeniem go przez osoby postronne.
8. Pierwszym podstawowym zabezpieczeniem danych jest używanie hasła przy rozpoczęciu pracy z komputerem, które nie jest zbyt proste: zawiera osiem znaków, jednocześnie małe i wielkie litery czy liczby, nie można go znaleźć w słowniku. Hasło powinno być zmieniane przez użytkownika przynajmniej raz na kwartał.
9. Nawet przy krótkim odejściu użytkownika komputera, na przykład po to by zrobić sobie kawę, jego komputer blokuje się i wymaga znów wpisania hasła; włączony jest zwykły wygaszacz ekranu. Hasło chroni dane znajdujące się na komputerze.
10. Hasła stosowane są też na niższych poziomach - opatrzone hasłem są pojedyncze pliki zawierające dane, takie jak arkusze kalkulacyjne z planami finansowymi czy bazy z danymi osobowymi.
11. Hasło jest skuteczne i tajne, nie jest podawane innym osobom i nie jest zapisywane w łatwo dostępnych miejscach.
16. Dane przesyłane w sieci, czy przechowywane w plikach są zaszyfrowane.
17. Z punktu widzenia zakresu posiadanych uprawnień dzieli się użytkowników na dwie grupy: aktywnych i biernych. Status "aktywnego" pozwala na pełną obsługę dostępnych funkcji, natomiast użytkownik "bierny" nie ma możliwości ingerencji w bazy danych pomimo formalnej dostępności do określonych funkcji systemu. Oznacza to, że osoby uprawnione do wykonywania tych samych funkcji programu różnią się zakresem dostępnych działań. Np. jedna z nich może zarówno dopisywać pozycje do katalogu kontrahentów lub korygować zawartość już istniejących, a druga tylko korygować dane, przy czym obie pozbawione są prawa do usuwania pozycji.
18. Operację kodowania dostępu do systemu dokonuje osoba instalująca i wdrażająca program, czyli Administrator.
19. Administratorem systemu jest informatyk obsługujący jednostkę.
20. Administrator systemu sporządził wykaz osób uprawnionych do pracy z systemem podając nazwisko, kod, hasło oraz uprawnienia (spis funkcji dostępnych) poszczególnych operatorów. Dostęp do tego typu dokumentu posiada Dyrektor CUW i korzysta z niego w sytuacjach awaryjnych, np. podczas nieobecności administratora.
21. W przypadku, gdy operator podczas wywoływania systemu poda zły symbol lub złe hasło, na ekranie pojawi się stosowny komunikat.

20. Jeśli podane hasło było prawidłowe, następuje sprawdzenie czy użytkownik o danym kodzie już nie pracuje w systemie.
21. Równolegle z ograniczeniami programowymi Administrator systemu steruje dostępem do systemu za pomocą mechanizmów zawartych w stosowanym oprogramowaniu sieciowym.
22. Istotnym problemem z punktu widzenia zachowania ciągłości pracy jest ochrona i właściwe przechowywanie przetwarzanych danych. 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 tworzy się kopie systemu, stanowiące jego replikę na dysku twardym, bądź na innym nośniku, np. płycie CD, dysku zewnętrznym. Kopiowanie odbywa się na inny dysk niż ten, na którym eksploatowany jest system, np. w przypadku sieci, gdy katalog bieżący znajduje się na dysku sieciowym. Częstotliwość wykonywania kopii awaryjnych pozostaje do uznania Administratora.
23. Jeżeli w czasie awarii nastąpi uszkodzenie lub zniszczenie zbiorów z danymi należy zwrócić się do producenta w celu ustalenia zakresu strat i przywrócenia funkcjonalności programu. Może zdarzyć się jednak, że jedynym rozwiązaniem staje się odzyskanie danych z kopii. Dlatego niezmiernie istotne jest częste sporządzanie tych kopii, co ogranicza do minimum konieczność powtórnego wprowadzania utraconych dokumentów. Operacja ta powinna być traktowana, jako ostateczność bowiem jej wykonanie równoznaczne jest z usunięciem zbiorów z katalogu z bieżącymi danymi.
24. System zabezpieczony jest przed wirusami. Instalowany jest systematycznie i aktualizowany program antywirusowy.
25. Kontrolę wewnętrzną środowiska informatycznego prowadzi Dyrektor CUW.
26. Kontrolę instytucjonalną w zakresie zabezpieczeń, oprogramowania, archiwizowania sprawuje informatyk obsługujący jednostkę.

Księgi rachunkowe prowadzone z użyciem komputera chronione są poprzez:		
1/ stosowanie odpornych na zagrożenia nośników danych:	tradycyjny nośnik informacji - wydruk komputerowy,	
	inne - na nośnikach komputerowych pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych – dysk zewnętrzny.	
2/ doborze stosownych środków ochrony zewnętrznej:	opracowane i przestrzegane są procedury chroniące księgi rachunkowe,	
	ochrona przed wirusami komputerowymi:	zakup programu antywirusowego (objęty opłatą licencyjną)
		regularne skanowanie zawartości komputera pod kątem występowania w nim wirusów, a w szczególności sprawdzanie przychodzącej poczty, sprawdzanie aktywnej treści przenikającej z sieci do komputera
3/ systematyczne tworzenie rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych, pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych:	na zewnętrznym dysku sieciowym NAS:	obowiązek tworzenia kopii bezpieczeństwa przez Administratora
4/ zapewnienie ochrony programów komputerowych i danych systemu informatycznego rachunkowości, poprzez stosowanie odpowiednich rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem:	przed instalacją oprogramowania sprawdza się, czy posiadany sprzęt komputerowy spełnia warunki stawiane przez producenta oprogramowania i czy działa on pod kontrolą odpowiednich wersji systemu operacyjnego i oprogramowania sieciowego	
	czynności instalacyjne, zleca się producentowi (dostawcy) oprogramowania lub wyspecjalizowanym służbom informatycznym	
	nie wolno instalować, ani używać oprogramowania, które nie zostało wcześniej dopuszczone do stosowania w jednostce	
	zmiany wersji systemu wprowadzane są wyłącznie przez wyspecjalizowane służby informatyczne	
	przed rozpoczęciem korzystania z programu pracownicy CUW zapoznają się z podręcznikiem użytkownika, dostarczonym przez producenta oprogramowania i bezwzględnie stosują zamieszczone tam polecenia oraz wskazówki	
	każdy użytkownik oprogramowania zobowiązany jest do przestrzegania reguł bezpieczeństwa opisanych w zarządzeniu Dyrektora CUW odnośnie zasad ochrony danych, programów i sprzętu informatycznego	
	stosuje się system podtrzymywania napięcia w razie awarii sieci energetycznej	
	monitory są usytuowane tak, aby uniemożliwiały odczytanie z nich chronionych danych przez osoby nieuprawnione	
	każda osoba przed dopuszczeniem do pracy przy chronionych danych zaznajamiana jest z przepisami dotyczącymi ich bezpieczeństwa	
	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 dotyczą	

28. Użytkownik, który uzyskał informacje lub sam stwierdził naruszenie zabezpieczeń chronionych danych zobowiązany jest niezwłocznie powiadomić o tym Administratora Danych Osobowych (ADO) – Dyrektora CUW lub IDO.
29. Inspektor Ochrony Danych (IOD) powinien w pierwszej kolejności:
    a) zapisać wszelkie informacje związane z danym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu bezpieczeństwa danych i czas samodzielnego wykrycia tego faktu.
    b) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu informatycznego na to pozwalają) wszystkie możliwe dokumenty i raporty, którego mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,
    c) przystąpić do zidentyfikowania rodzaju zdarzenia, zwłaszcza skali zniszczeń i metody dostępu do danych intruza.
30. Niezwłocznie podjąć odpowiednie kroki w celu powstrzymania i ograniczenia dostępu do danych przez osoby niepowołane, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji.
31. Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych w systemie.
32. IOD powinien sprawdzić:
    a) stan urządzeń wykorzystywanych do przetwarzania chronionych danych,
    b) zawartość zbioru chronionych danych,
    c) sposób działania programu.
33. Po dokonaniu powyższych czynności IOD powinien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującego identyfikację:
    a) rodzaj zaistniałego zdarzenia,
    b) metody dostępu do chronionych danych intruza,
    c) skali zniszczeń.
34. Niezwłocznie należy przywrócić normalny stan działania systemu, przy czym jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest jej odtworzenie z ostatniej kopii bezpieczeństwa z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu przez intruza tą samą drogą.
35. 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:

a) Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej, należy przeprowadzić dodatkowe szkolenie z zakresu bezpieczeństwa, wszystkich osób mających dostęp do chronionych danych.
b) Jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy znaleźć źródło jego pochodzenia i wykonać niezbędne działania w celu pozbycia się jego.
c) 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.
d) Jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej (użytkownika), należy wyciągnąć konsekwencje regulowane ustawą.
e) W przypadku kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy należy powiadomić o fakcie najbliższy komisariat policji.
f) Jeżeli przyczyną zdarzenia był zły stan techniczny sprzętu lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo - programowe.

36. IOD przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i przekazuje do ADO.

2. Przechowywanie zbiorów

1. Dokumentacje: księgi rachunkowe, dowody księgowe, dokumenty inwentaryzacyjne i sprawozdania finansowe przechowywane są w należyty sposób i chronione przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem.
2. 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.
3. Dowody księgowe po ich zaksięgowaniu gromadzone są w segregatorach, oznakowanych rodzajem gromadzonych dowodów, rokiem którego dotyczą.
4. Roczne zbiory dowodów księgowych i dokumentów inwentaryzacyjnych oznacza się określeniem nazwy ich rodzaju oraz symbolem końcowych lat.

5. Po zatwierdzeniu sprawozdania finansowego za dany rok obrotowy, dokumentację przyjętych zasad rachunkowości, księgi rachunkowe oraz sprawozdania finansowe, w tym również sprawozdanie z działalności jednostki, przechowuje się odpowiednio:
   1/ Zatwierdzone roczne sprawozdania finansowe podlegają przechowywaniu przez okres co najmniej 5 lat, licząc od początku roku następującego po roku obrotowym, w którym zatwierdzono sprawozdanie finansowe.
   2/ Pozostałe zbiory przechowuje się co najmniej przez okres:
      a. księgi rachunkowe – 5 lat;
      b. karty wynagrodzeń pracowników bądź ich odpowiedniki – przez okres wymaganego dostępu do tych informacji, wynikający z przepisów emerytalnych, rentowych oraz podatkowych, nie krócej jednak niż 5 lat;
      c. dowody księgowe dotyczące wpływów ze sprzedaży detalicznej – do dnia zatwierdzenia sprawozdania finansowego za dany rok obrotowy, nie krócej jednak niż do dnia rozliczenia osób, którym powierzono składniki aktywów objęte sprzedażą detaliczną;
      d. dowody księgowe dotyczące środków trwałych w budowie, pożyczek oraz umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym lub objętych postępowaniem karnym albo podatkowym – przez 5 lat od początku roku następującego po roku obrotowym, w którym operacje, transakcje i postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione;
      e. dokumentację przyjętego sposobu prowadzenia rachunkowości – przez okres nie krótszy od 5 lat od upływu jej ważności;
      f. dokumenty dotyczące rękojmi i reklamacji – 1 rok po terminie upływu rękojmi lub rozliczeniu reklamacji;
      g. dokumenty inwentaryzacyjne – 5 lat;
      h. pozostałe dowody księgowe i sprawozdania, których obowiązek sporządzenia wynika z ustawy – 5 lat.
6. Okresy przechowywania ustalone w pkt 5 oblicza się od początku roku następującego po roku obrotowym, którego dane zbiory dotyczą.

3. Udostępnianie danych i dokumentów

1. Udostępnienie osobie trzeciej zbiorów lub ich części:
   1) do wglądu na terenie jednostki - wymaga zgody Dyrektora CUW,

2) poza siedzibą jednostki - wymaga pisemnej zgody Dyrektora CUW oraz pozostawienia w jednostce potwierdzonego spisu przejętych dokumentów, chyba że odrębne przepisy stanowią inaczej.