Załącznik nr 1.6
do Zarządzenia nr 46.2018
Dyrektora Częstochowskiego
Centrum Świadczeń
z dnia 14.05.2018 r.

ZASADY OCHRONY DANYCH W CZĘSTOCHOWSKIM CENTRUM ŚWIADCZEŃ

§ 1.
Przechowywanie i ochrona danych

Dokumentację opisującą zasady (politykę) rachunkowości, księgi rachunkowe, dowody księgowe, dokumenty inwentaryzacyjne, sprawozdania budżetowe i finansowe należy przechowywać w należyty sposób i chronić przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem.

Sposób przechowywania dokumentacji powinien zapewniać:

1) nienaruszalność (integralność) danych, które powinny być kompletne i poprawne oraz chronione przed mimowolnymi lub celowymi niewłaściwymi zmianami;
2) poufność danych, które nie powinny być przekazywane osobom do tego nieupoważnionym lub upubliczniane;
3) autoryzację danych, do których dostęp mają uprawnione do tego osoby.

Fizyczne zabezpieczenie zewnętrzne zapewnia ochronę przed dostępem osób nieupoważnionych do następujących elementów systemu rachunkowości i dokumentacji:

1) sprzętu komputerowego wspomagającego księgowość;
2) księgowego systemu informatycznego;
3) kopii zapasowych zapisów księgowych;
4) zasad rachunkowości;
5) ksiąg rachunkowych;
6) dowodów księgowych;
7) dokumentacji inwentaryzacyjnej;
8) sprawozdań budżetowych i finansowych.

4. Dowody księgowe i dokumenty inwentaryzacyjne przechowuje się w **Centrum** w oryginalnej postaci, w ustalonym porządku dostosowanym do sposobu prowadzenia ksiąg rachunkowych, w podziale na okresy sprawozdawcze, w sposób pozwalający na ich łatwe odszukanie.

§ 2.
Przechowywanie i ochrona danych przetwarzanych przy użyciu komputera

Dla prawidłowej ochrony ksiąg rachunkowych prowadzonych przy użyciu komputera stosowane są:

1) nośniki danych odporne na zagrożenia;
2) systematycznie tworzone - rezerwowe kopie zbiorów danych zapisanych na trwałych nośnikach informacji;
3) programy komputerowe i dane informatycznego systemu rachunkowości chronione przed dostępem osób nieupoważnionych i zniszczeniem poprzez zastosowanie właściwych rozwiązań organizacyjnych i programowych.

Ochrona przed nieupoważnionym dostępem do bazy danych w programach komputerowych polega na:

1) nadawaniu użytkownikom praw dostępu do sieci komputerowej z restrykcjami czasowymi (w określonych dniach tygodnia, w określonych godzinach);
2) systemie haseł, których okresowa zmiana wymuszana jest przez system niezależnie od blokowania dostępu po 3-krotnym błędnym wpisaniu hasła;
3) kontroli grupy, do której musi należeć użytkownik, by w czasie logowania system przydzielił odpowiednie zasoby i zmapował dyski sieciowe;
4) nadawaniu dostępu do aplikacji poprzez system uprawnień (uprawnienia dotyczą nie tylko możliwości uruchomienia samej aplikacje, lecz także – niezależnie – poszczególnych jej funkcji).

Ochrona przed zdarzeniami losowymi:

1) wykonywanie kopii danych na innych dyskach twardych przez administratora sieci (backup) pełny backup bazy danych w cyklu dziennym, backup log bazy danych w cyklu dziennym z częstotliwością od 2 do 4 godzin w czasie pracy **Centrum**;
2) odłączenie komputerów do wydzielonej – dedykowanej sieci komputerowej posiadającej centralny UPS;

3) niezależne podtrzymywanie zasilania serwerów przez UPS-y;
4) profilaktyka antywirusowa, stała aktualizacja programów zabezpieczających.

Kopie bezpieczeństwa systemu sporządzane są przez administratora systemu. W celu zapewnienia jak najwyższego stopnia bezpieczeństwa przechowywanych w bazie SQL danych przyjęto tworzenie na bieżąco kopii baz.

Zbiory danych tworzących księgi rachunkowe na komputerowych nośnikach danych są na dzień kończący okresy obrachunkowe kopiowane na płyty CD lub DVD i przechowywane w **Zespole d/s Informatyki.**

Ochrona przed zdarzeniami losowymi danych informatycznych określa odrębne zarządzenie w sprawie wprowadzenia Polityki Bezpieczeństwa Centrum oraz wyznaczenia Administratora Bezpieczeństwa Informacji.

§ 3.

Okresy przechowywania danych

1. Trwałemu przechowywaniu podlegają roczne sprawozdania finansowe **Centrum**.

2. Okresowe przechowywanie - terminy oblicza się od początku roku następującego po roku obrotowym, którego dane zbiory (dokumenty), dotyczą:
1) księgi rachunkowe, dokumenty inwentaryzacyjne, pozostałe dowody księgowe i dokumenty – 5 lat;
2) karty wynagrodzeń pracowników bądź ich odpowiedniki - przez okres wymaganego dostępu do tych informacji wynikający z przepisów emerytalnych, rentowych i podatkowych, nie krócej jednak niż 50 lat;
3) dowody księgowe dotyczące środków trwałych w budowie, pożyczek, roszczeń dochodzonych w postępowaniu cywilnym, karnym i podatkowym - przez 5 lat od początku roku następującego po roku obrotowym, w którym operacje i postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione;
4) dokumentację przyjętego sposobu prowadzenia rachunkowości - przez okres nie krótszy niż 5 lat od upływu ich ważności.

3. Okresy przechowywania danych określa zarządzenie Dyrektora Centrum w sprawie wprowadzenia jednolitego rzeczowego wykazu akt w Centrum Świadczeń w Częstochowie, o ile przepisy szczególne nie stanowią inaczej.

§ 4.

Udostępnianie danych i dokumentów

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

1) w siedzibie Centrum do wglądu po uzyskaniu zgody Dyrektora Centrum lub upoważnionej przez niego osoby;
2) poza siedzibą **Centrum** po uzyskaniu pisemnej zgody Dyrektora Centrum i pozostawieniu pisemnego potwierdzenia zawierającego spis wydanych dokumentów.