**ZARZĄDZENIE NR 58/2021**

**BURMISTRZA MIASTA I GMINY CHORZELE**

z dnia 30 marca 2021 r.

**w sprawie wyznaczenia Administratora Systemu Teleinformatycznego oraz Inspektora Bezpieczeństwa Teleinformatycznego w Urzędzie Miasta i Gminy w Chorzelach**

na podstawie art. 52 ust.1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) oraz § 13 i 14 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r., Nr 159, poz. 948 ) zarządzam co następuje:

§1

Wyznacza się Pana Roberta Osowskiego na Administratora Systemu Teleinformatycznego „Bezpiecznego Stanowiska Komputerowego” w Urzędzie Miasta i Gminy w Chorzelach, w których przetwarzane są informacje niejawne o klauzuli „zastrzeżone” w Urzędzie Miasta i Gminy w Chorzelach. Zakres zadań Administratora Systemu Teleinformatycznego określa załącznik nr 1 do niniejszego zarządzenia.

§2

Wyznacza się Panią Marię Bądkowską do pełnienia funkcji Inspektora Bezpieczeństwa Teleinformatycznego systemu, w których przetwarzane są informacje niejawne o klauzuli „zastrzeżone” w Urzędzie Miasta i Gminy w Chorzelach. Zakres zadań Inspektora Bezpieczeństwa Teleinformatycznego określa załącznik nr 2 do niniejszego zarządzenia.

§3

Wykonanie Zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnych w Urzędzie Miasta i Gminy w Chorzelach.

§4

Zarządzenie wchodzi z życie z dniem podpisania.

Burmistrz Miasta i Gminy Chorzele

Beata Szczepankowska

*Załącznik nr 1 do*

*Zarządzenia nr 58/2021*

*Burmistrza Miasta i Gminy Chorzele*

*z dnia 30 marca 2021*

* + - 1. **Do zadań Administratora Systemu należy w szczególności:**

1. odpowiedzialność za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego
2. obsługa techniczna systemu,
3. sprawdzanie poprawności działania systemu,
4. przydzielanie haseł dostępowych użytkownikom systemu,
5. zapewnienie, aby wszyscy użytkownicy systemu stosowali się do Procedur Bezpieczeństwa,
6. utrzymanie i aktualizacja list autoryzowanych użytkowników systemu,
7. nadzorowanie użytkowników systemu BSK,
8. zapewnienie przestrzegania Szczegółowych Wymagań Bezpieczeństwa,
9. doradzanie użytkownikom w zakresie bezpieczeństwa teleinformatycznego,
10. wdrażanie procedur ochrony antywirusowej,
11. opracowywanie planów awaryjnych i planu naprawy systemu teleinformatycznego,
12. ochrona niejawnych wydruków systemu wyprowadzanych na urządzenia wyjściowe, zgodnie z obowiązującymi w tym zakresie procedurami,
13. prowadzenie kontroli dotyczących obecności klasyfikowanych mediów magnetycznych i poprawności ich opisu oraz utrzymywanie ewidencji   
    tych sprawdzeń,
14. sprawdzenie i zapewnienie by niejawne odpady były niszczone w regularnych odstępach czasu, zgodnie z unormowaniami w tym zakresie,
15. proponowanie zmian do Szczególnych Warunków Bezpieczeństwa i Procedur Bezpiecznej Eksploatacji mających na celu poprawę stanu bezpieczeństwa systemu,
16. powiadamianie Pełnomocnika ds. Ochrony Informacji Niejawnych oraz Inspektora Bezpieczeństwa Teleinformatycznego o wszelkich wykrytych naruszeniach i zagrożeniach systemu,
17. prowadzenie Dziennika Pracy w Systemie BSK.

*Załącznik nr 2 do*

*Zarządzenia nr 58/2021*

*Burmistrza Miasta i Gminy Chorzele*

*z dnia 30 marca 2021*

1. **Do zadań Inspektora Bezpieczeństwa Teleinformatycznego należy w szczególności:**
2. odpowiedzialność za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa (SWBS) oraz kontrolę przestrzegania procedur bezpiecznej eksploatacji (PBE).,
3. zapewnienie, aby wszyscy użytkownicy Systemu BSK posiadali stosowne dopuszczenia oraz byli przeszkoleni w zakresie Szczegółowych Wymagań Bezpieczeństwa,
4. zapewnienie przestrzegania zasad ochrony informacji niejawnych, przetwarzanych, przechowywanych i przesyłanych w systemie lub sieci teleinformatycznej, w tym właściwego obiegu dokumentów (wchodzących, wychodzących i nośników informacji),
5. przygotowanie i uaktualnianie „Wykazu osób zapoznanych z Procedurami Bezpieczeństwa”, który podpisywany jest przez wszystkich użytkowników systemu BSK,
6. doradzanie użytkownikom w zakresie bezpieczeństwa teleinformatycznego,
7. utrzymanie bieżącego schematu obszaru podlegającymi nadzorowi i przekładanie jego kopii do Pełnomocnika ds. Ochrony Informacji Niejawnych,
8. wszelkie produkty systemu, które nie mogą być jednoznacznie określone   
   lub zawierają dane uboczne powinny być kierowane do Pełnomocnika ds. Ochrony Informacji Niejawnych, dane te obejmują np. podejrzane urządzenia, które zostały dodane do systemu przez nieznane osoby lub nieznane oprogramowanie,
9. organizacja szkolenia użytkowników w zakresie ochrony informacji niejawnych przetwarzanych, przechowywanych i przesyłanych w funkcjonującym w jednostce systemie teleinformatycznym,
10. nadzór nad konfiguracją systemu, przemieszczaniem sprzętu oraz nad prowadzeniem jego ewidencji,
11. proponowanie zmian do Szczególnych Warunków Bezpieczeństwa i Procedur Bezpiecznej Eksploatacji mających na celu poprawę stanu bezpieczeństwa systemu,
12. informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych o wszelkich wykrytych naruszeniach i zagrożeniach systemu,
13. prowadzenie Dziennika Pracy w Systemie BSK.