

**ZARZĄDZENIE NR 39**  
**BURMISTRZA MIASTA ŻARÓW**

z dnia 9 marca 2021 r.

**w sprawie zatwierdzenia dokumentacji bezpieczeństwa systemu teinformatycznego w Urzędzie Miejskim w Żarowie i udzielenia akredytacji bezpieczeństwa dla systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe (BSK)” przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”.**

Na podstawie art. 48 ust. 9 i art. 52 ust. 1 ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz. U. z 2019r. poz. 742) oraz Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011r. Nr 159 poz. 948) zarządzam, co następuje:

**§ 1.** Zatwierdzam dokumentację bezpieczeństwa systemu teleinformatycznego do przetwarzania informacji niejawnych:

- 1) „Procedury Bezpiecznej Eksploatacji Systemu Teleinformatycznego – Bezpieczne Stanowisko Komputerowe BSK, stanowiące załącznik nr 1 do niniejszego zarządzenia,
- 2) „Szczególne Wymagania Bezpieczeństwa Systemu Teleinformatycznego - Bezpieczne Stanowisko Komputerowe BSK” , stanowiące załącznik nr 2 do niniejszego zarządzenia.

**§ 2.** Udzielam akredytacji bezpieczeństwa teleinformatycznego na okres 5 lat dla systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe BSK” w Urzędzie Miejskim w Żarowie przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”.

**§ 3.** Wszystkich użytkowników systemu teleinformatycznego zobowiązuję do ścisłego przestrzegania dokumentacji bezpieczeństwa określonej w§1 zarządzenia.

**§ 4.** Dokumentację systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe BSK”, aktualizuje i przechowuje Pełnomocnik ds. Ochrony Informacji Niejawnych.

**§ 5.** Wyznaczam osoby odpowiedzialne za planowanie, wdrażanie i eksploatację systemu teleinformatycznego „Bezpieczne Stanowisko Komputerowe BSK”:

- 1) Administrator Systemu – Marcin Wolfram
- 2) Inspektor Bezpieczeństwa Teleinformatycznego – Leszek Buchowski
- 3) Pełnomocnik ds. Ochrony Informacji Niejawnych – Michał Domański.

**§ 6.** Do zadań Administratora należy:

- 1) instalacja systemu i przydział uprawnień użytkownikom,
- 2) szkolenie użytkowników z zasad korzystania systemu teleinformatycznego , obsługa techniczna systemu , okresowe sprawdzanie zabezpieczeń,
- 3) wdrażanie procedur bezpieczeństwa i procedur ochrony antywirusowej,
- 4) informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych o stwierdzonych naruszeniach bezpieczeństwa systemu oraz wykrytych wirusach.

**§ 7.** Do zadań Inspektora Bezpieczeństwa Teleinformatycznego należy:

- 1) nadzór nad konfiguracją systemu,
- 2) kontrola przestrzegania procedur bezpiecznej eksploatacji,
- 3) kontrola zabezpieczeń systemu teleinformatycznego.

**§ 8.** Do zadań Pełnomocnika ds. Ochrony Informacji Niejawnych należy:

- 1) zapewnienie zasad przestrzegania ochrony informacji przetwarzanych, przechowywanych w systemie teleinformatycznym,
- 2) nadzór nad właściwym obiegiem dokumentów niejawnych i nośników informacji,

3) zapewnienie bezpieczeństwa fizycznego obszaru, w którym usytuowany jest system teleinformatyczny,

4) zapewnienie dostępu do systemu teleinformatycznego wyłącznie osobom mającym uprawnienia.

§ 9. Użytkownicy systemu przed uzyskaniem fizycznego dostępu do systemu teleinformatycznego są zobowiązani odbyć dodatkowe szkolenie w zakresie jego funkcjonowania oraz zasad zapewnienia warunków ochrony informacji niejawnych przetwarzanych w systemie.

§ 10. Szkolenia prowadzone są przez Pełnomocnika ds. Informacji Niejawnych i Administratora Systemu.

§ 11. Wszyscy użytkownicy Systemu Teleinformatycznego – „Bezpieczne Stanowisko Komputerowe BSK” , ponoszą odpowiedzialność za wszelkie naruszenia obowiązującego prawa w trakcie korzystania z systemu.

§ 12. Wykonanie zarządzenia powierza się Pełnomocnikowi ds. Informacji Niejawnych.

§ 13. Zarządzenie wchodzi w życie z dniem podpisania.