ZARZĄDZENIE Nr 13/2016
WÓJTA - KIEROWNIKA URZĘDU GMINY
z dnia 23 listopada 2016 roku

w sprawie zmiany Regulaminu Organizacyjnego Urzędu Gminy w Drzycimiu.

Na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2016 r. poz. 902) oraz § 7 ust. 8 Regulaminu Organizacyjnego Urzędu Gminy w Drzycimiu zarządzam co następuje:

§ 1. Treść § 7 ust. 3 otrzymuje brzmienie:
„Pion ochrony informacji niejawnych (PO)
1) pełnomocnik ochrony w zakresie ochrony informacji niejawnych, kierujący pionem ochrony, podległy bezpośrednio kierownikowi jednostki organizacyjnej;
2) kierownik kancelarii niejawnej;
3) inspektor bezpieczeństwa teleinformatycznego."

§ 2. Dodaje się § 7 ust. 3a:
„Administrator systemów teleinformatycznych (AST)."

§ 3. Rozdział VII otrzymuje brzmienie:
„Organizacja Pionu ochrony informacji niejawnych, ochrony systemów teleinformatycznych i ochrony danych osobowych"

§ 4. Treść § 27 ust. 2 pkt 3 otrzymuje brzmienie:
„Inspektor BTI realizuje zadania w zakresie bieżącej kontroli zgodności funkcjonowania systemu teleinformatycznego z dokumentacją bezpieczeństwa TI. Kontrole Inspektora BTI powinny odbywać się nie rzadziej niż raz na kwartał. Inspektor BTI w szczególności kontroluje:

a) przestrzeganie zasad ochrony informacji niejawnych w systemie teleinformatycznym;
b) stan zabezpieczeń fizycznych, elektromagnetycznych i elektronicznych pomieszczenia, w którym usytuowany jest system teleinformatyczny;
c) aktualność wykazów osób mających dostęp do systemu teleinformatycznego, przydzielanie kont użytkownikom, zakres nadanych im uprawnień oraz prawidłowość zabezpieczeń zastosowanych w systemie;
d) znajomość i przestrzeganie przez użytkowników procedur bezpiecznej eksploatacji systemu teleinformatycznego;
e) przestrzeganie zasad i wymagań w zakresie oznaczania, ewidencjonowania, przechowywania i przekazywania wytworzonych dokumentów niejawnych oraz ich terminowe rozliczanie;
f) zgodność konfiguracji systemu teleinformatycznego z dokumentacją bezpieczeństwa teleinformatycznego;
g) przeprowadza okresowe kontrole elektronicznych nośników informacji używanych w systemie, poprawności ich opisu oraz utrzymuje ewidencję tych kontroli;
h) uczestniczy w corocznej analizie ryzyk, prowadzi szkolenia z zakresu eksploatacji i bezpieczeństwa systemu TI;
i) analizuje rejestr zdarzeń w systemie teleinformatycznym;
j) informuje pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu teleinformatycznego;

k) prowadzi szkolenia użytkowników w zakresie ochrony informacji niejawnych oraz przestrzegania zasad bezpieczeństwa w systemie lub sieci teleinformatycznej;
l) wszelkie modyfikacje i prace związane z systemem odnotowuje w „Dzienniku pracy systemu".

§ 5. Z § 27 ust. 2 usuwa się pkt 4) i 5).

§ 6. Dodaje się § 27a o treści:
„Administrator systemu TI realizuje zadania w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad bezpieczeństwa systemu TI, a w szczególności odpowiada za:

1) comiesięczną obsługę techniczną systemu;
2) sprawdzenie poprawności działania systemu;
3) opracowywanie projektów SWB systemu teleinformatycznego oraz propozycji ich uaktualnienia, uczestniczenie w corocznej analizie ryzyk;
4) wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemu teleinformatycznego;
5) wdrażanie procedur ochrony antywirusowej oraz na bieżąco aktualizuje bazę wirusów programu antywirusowego ;
6) opracowanie planów napraw systemu teleinformatycznego;
7) informowanie pełnomocnika ochrony oraz inspektora bezpieczeństwa o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego oraz wykrytych wirusach;
8) proponowanie zmian mających na celu poprawę bezpieczeństwa systemu teleinformatycznego;

a ponadto:

1) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu komputerowego;
2) upewnia się, czy cały personel posiadający dostęp do systemu komputerowego posiada stosowne poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych – w przypadku dostępu do systemu komputerowego osób nieposiadających stosownych dopuszczeń, zapewnia odpowiednie zabezpieczenie systemu komputerowego;
3) prowadzi osobiście lub nadzoruje profilaktykę antywirusową systemu komputerowego;
4) prowadzi nadzór sprzętu oraz oprogramowania pod kątem kontroli nieuprawnionych zmian ich konfiguracji;
5) dokonuje wszelkich zmian w konfiguracji sprzętu lub oprogramowania mających wpływ na bezpieczeństwo systemu komputerowego;
6) dokonuje analizy zgłoszonych przypadków incydentów infekcji wirusowych lub innych, wskazujących na nieautoryzowane próby ingerencji w systemie bezpieczeństwa oraz w zależności od stopnia zagrożenia funkcjonowania systemu bezpieczeństwa, podejmuje odpowiednie kroki zaradcze zapewnienie strategii, uregulowań i procedur bezpieczeństwa;
7) prowadzi szkolenia użytkowników z zakresu bezpieczeństwa systemu komputerowego lub występuje z wnioskiem o przeprowadzenie szkolenia użytkowników z zakresu bezpieczeństwa systemu komputerowego;
8) doskonali się z zakresu wiedzy o bezpieczeństwie systemu komputerowego
9) dokonuje analizy zagrożeń oraz ryzyka i melduje do Pionu Ochrony o wszelkich wykrytych lukach, naruszeniach i zagrożeniach.
10) wszelkie modyfikacje i prace związane z systemem odnotowuje w „Dzienniku pracy systemu".

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY DRZYCIM

mgr Waldemar Moczyński