ZARZĄDZENIE NR 51 / 2021
WÓJTA GMINY OROŃSKO
z dnia 2 czerwca 2021 roku

w sprawie powołania „Pionu Ochrony Informacji Niejawnych" w Urzędzie Gminy w Orońsku oraz wyznaczenia Inspektora Bezpieczeństwa Teleinformatycznego i Administratora Systemu Informatycznego

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t. j. Dz. U. 2020 poz. 713 ze zm.) w związku z art. 14 ust. 1, art. 15 ust. 2 i ust. 4, art. 16, art. 52 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (t. j. Dz. U. 2019 poz. 742 ze zm.) oraz § 13 i § 14 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 2011 nr 159 poz. 948), zarządzam co następuje:

§1.

1. W celu zapewnienia właściwej ochrony informacji niejawnych w Urzędzie Gminy w Orońsku, powołuje „Pion Ochrony Informacji Niejawnych", zwany dalej „pionem ochrony".
2. Pion ochrony podlega Pełnomocnikowi do spraw ochrony informacji niejawnych.

§2.

W skład pionu ochrony wchodzą:

1. Pełnomocnik do spraw ochrony informacji niejawnych.
2. Inspektor Bezpieczeństwa Teleinformatycznego.
3. Administrator Systemu Informatycznego.

§3.

Z dniem 2 czerwca 2021 roku wyznaczam do pełnienia funkcji Inspektora Bezpieczeństwa Teleinformatycznego **Pana Dariusza Tomczyka.**

§4.

Z dniem 2 czerwca 2021 roku wyznaczam do pełnienia funkcji Administratora Systemu Informatycznego **Pana Dariusza Kaczora**.

§5.

Ww. pracownicy posiadają odpowiednie uprawnienia do pełnienia przypisanych im funkcji o których mowa w ustawie o ochronie informacji niejawnych.

§6.

Pracownicy pionu ochrony podlegają Pełnomocnikowi do spraw ochrony informacji niejawnych.

§7.

Zadania Pełnomocnika do spraw ochrony informacji niejawnych określa ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (t. j. Dz. U. 2019 poz. 742 ze zm.) oraz akty wykonawcze do tej ustawy.

§8.

Inspektor Bezpieczeństwa Teleinformatycznego realizuje zadania w zakresie weryfikacji i bieżącej kontroli zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji, bierze udział w procesie zarządzania ryzykiem systemie teleinformatycznym weryfikując:

1. przestrzeganie zasad ochrony przetwarzanych w systemie teleinformatycznym informacji niejawnych;
2. poprawność realizacji zadań wykonywanych przez administratora systemu teleinformatycznego;
3. właściwe zarządzanie konfiguracją systemu teleinformatycznego oraz uprawnieniami przydzielanymi użytkownikom;
4. znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, w tym w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;
5. stan zabezpieczeń systemu teleinformatycznego, w tym analizując rejestry zdarzeń systemu teleinformatycznego;
6. aktualność wykazów osób mających dostęp do systemu teleinformatycznego;

Ponadto inspektor bezpieczeństwa teleinformatycznego:

1. uczestniczy w opracowywaniu programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów teleinformatycznych.

§9.

Administrator Systemu Informatycznego jest odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, a w szczególności:

1. bierze udział w opracowaniu i aktualizowaniu dokumentacji bezpieczeństwa systemu teleinformatycznego;
2. przechowuje oryginały zatwierdzonej dokumentacji bezpieczeństwa systemu teleinformatycznego;
3. bierze udział w procesie zarządzania ryzykiem w systemie teleinformatycznym;
4. szkoli użytkowników systemu teleinformatycznego z zakresu procedur bezpiecznej eksploatacji;
5. utrzymuje zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;
6. wdraża zabezpieczenia w systemie teleinformatycznym oraz procedury bezpiecznej eksploatacji;
7. systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń i poprawność działania systemu teleinformatycznego;
8. analizuje i archiwizuje rejestr zdarzeń w systemie teleinformatycznym;
9. zapewnia dostęp do systemu teleinformatycznego wyłącznie użytkownikom posiadającym wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa lub upoważnienie.
10. przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki (komórki) organizacyjnej;
11. prowadzi wykaz osób mających dostęp do systemu teleinformatycznego zawierający, co najmniej:
    - imię i nazwisko;
    - nazwę jednostki (komórki) organizacyjnej;
    - posiadane poświadczenie bezpieczeństwa lub upoważnienie (jego numer, klauzulę i datę ważności);

12. odpowiada za tworzenie kopii bezpieczeństwa plików;
13. przeprowadza czynności serwisowe w przypadku awarii sprzętu;
14. prowadzi dokumentację eksploatacyjną systemu - „Dziennik działań Administratora Systemu Teleinformatycznego";
15. współpracuje z Kierownikiem Kancelarii Materiałów Niejawnych nad wydawaniem i przechowywaniem elektronicznych nośników danych;
16. informuje pełnomocnika ochrony o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego;
17. zgłasza do pełnomocnika ochrony potrzeby w zakresie serwisowania i certyfikacji środków ochrony elektromagnetycznej.

§10.

Wykonanie zarządzenia powierzam Pełnomocnikowi do spraw ochrony informacji niejawnych.

§11.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Henryk Nosowski