LUBUSKI WOJEWÓDZKI INSPEKTOR
NADZORU BUDOWLANEGO
ul. Kosynierów Gdyńskich 75
66-400 Gorzów Wlkp.

ZARZĄDZENIE NR 9/15

Lubuskiego Wojewódzkiego Inspektora Nadzoru Budowlanego

z dnia 21 kwietnia 2015r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych oraz powołania Administratora Bezpieczeństwa Informacji w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Gorzowie Wlkp.

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz 18 pkt 1 Regulaminu Organizacyjnego Wojewódzkiego Inspektoratu Nadzoru Budowlanego w Gorzowie Wlkp., ustalonego zarządzeniem nr 1/15 Lubuskiego Wojewódzkiego Inspektora Nadzoru Budowlanego z dnia 05 lutego 2015r. w sprawie ustalenia regulaminu organizacyjnego Wojewódzkiego Inspektoratu Nadzoru Budowlanego w Gorzowie Wlkp. zarządzam, co następuje:

§ 1. Wprowadza się Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Gorzowie Wlkp., która stanowi załącznik nr 1 do niniejszego zarządzenia.

§2. Powołuje Pana Grzegorz Małyszek na Administratora Bezpieczeństwa Informacji (ABI) w Wojewódzkim Inspektoracie Nadzoru Budowlanego w Gorzowie Wlkp.

§3. Zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji określa załącznik do niniejszego zarządzenia.

§4. Zarządzenie wchodzi w życie z dniem podpisania.

Lubuski Wojewódzki Inspektor
Nadzoru Budowlanego
(-)
Agnieszka Harasimowicz

Obowiązki Administratora Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji odpowiada w szczególności za:

1. poprawność i aktualizację dokumentacji (polityki bezpieczeństwa, instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych);
2. kontrole stanu wydanych upoważnień oraz ewidencji osób upoważnionych;
3. prowadzenie sprawdzania stanu bezpieczeństwa i sporządzanie propozycji zmian;
4. kontrole poprawności stosowania procedur dotyczących ochrony danych osobowych przez wszystkie upoważnione osoby;
5. realizowanie obowiązków związanych z zabezpieczeniem danych w systemach informatycznych.

Wymieniony wyżej zakres odpowiedzialności administratora bezpieczeństwa informacji sprawia, że do jego najważniejszych obowiązków należą m.in.:

1. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.
2. Dopilnowanie, aby komputery przenośne, w których przetwarzane są dane osobowe, były zabezpieczone hasłem dostępu przed nieautoryzowanym uruchomieniem.
3. Nadzór nad naprawami, konserwacją oraz likwidacja urządzeń komputerowych, na których zapisane są dane osobowe.
4. Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
5. Sprawdzanie systemu pod kątem obecności wirusów komputerowych, wykonywanie aktualizacji systemów antywirusowych i ich konfiguracja.
6. Wykonywanie kopii awaryjnych, ich przechowywanie oraz ich okresowe przeglądanie pod kątem ich dalszej przydatności.
7. Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe, który obejmuje ustalenie identyfikatorów użytkowników i ich haseł.
8. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działanie programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych, a następnie przedstawienie administratorowi danych ewentualnych zmian do instrukcji zarządzania systemem informatycznym w celu wyeliminowania przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych.
9. Śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i wdrażanie takich narzędzi, metod pracy oraz sposobów zarzadzania systemem informatycznym, które bezpieczeństwo to wzmocnią.