

Zakres Obowiązków Administratora Bezpieczeństwa Informacji

Administrator bezpieczeństwa informacji odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób nie powołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

Do jego głównych obowiązków należy:

1. Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany.
2. Nadzór czynności związanych ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych i uaktualnianiem systemów antywirusowych i ich konfiguracji.
3. Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
4. Nadzór nad przeglądami, naprawami, konserwacją oraz likwidacją urządzeń komputerowych a także aktualizacją systemów służących do przetwarzania danych osobowych.
5. Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.
6. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny.
7. Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych. Nadzorowanie, o którym mowa wyżej powinno obejmować: ustalenie identyfikatorów użytkowników i ich haseł, dopilnowanie aby hasła użytkowników były zmieniane co najmniej raz na miesiąc, dopilnowanie aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła, dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy /również po upływie terminu ich ważności/, dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zostały natychmiast wyrejestrowane z systemu, a ich hasła unieważnione.
8. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania.
9. Dopilnowanie, aby komputery przenośne, w których przetwarzane są dane

osobowe zabezpieczone były hasłem dostępu przed nieupoważnionym dostępem.

10. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych.
11. Analizowanie sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych /jeśli takie wystąpiło/ oraz przygotowanie i przedstawienie administratorowi danych takich zmian do instrukcji zarządzania systemem informatycznym, które wyeliminują lub ograniczą w przyszłości podobne przypadki.

Niezależnie od wymienionych wyżej czynności, obowiązkiem administratora bezpieczeństwa informacji jest śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo danych przetwarzanych w tym systemie wzmocnią.