WÓJT GMINY
w Brodach

Zarządzenie Nr 106/2013

Wójta Gminy Brody

z dnia 22 lipca 2013 roku

w sprawie: wyznaczenia Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Brodach.

Na podstawie art. 36 ust. 3 ustawy z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) zarządzam co następuje:

§ 1.

Wyznaczam Pana Łukasza Wzorka na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy Brody.

§ 2.

Obowiązki Administratora Bezpieczeństwa Informacji określa załącznik do niniejszego zarządzenia.

§ 3.

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
Gminy Brody
mgr Andrzej Krzygoda

Załącznik
do Zarządzenia Wójta Gminy Brody
Nr 106/2013 z dnia 22 lipca 2013r.

Obowiązki Administratora Bezpieczeństwa Informacji

1. Utworzenie oraz prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych, tj. wypracowanych w Urzędzie Gminy w Brodach dokumentów dotyczących Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe, oraz kontrolą przebywających w nich osób. Pomieszczenia, o których mowa wyżej, powinny być zabezpieczone przed dostępem do nich osób nieposiadających uprawnień do przetwarzania danych osobowych. Osoby nieposiadające takich uprawnień mogą przebywać w nich jedynie w obecności osób uprawnionych. Na czas nieobecności zatrudnionych tam osób, pomieszczenia te powinny być odpowiednio zabezpieczone. W celu zabezpieczenia pomieszczeń należy zastosować odpowiednie zamki do drzwi oraz sprawować właściwy nadzór nad kluczami do tych pomieszczeń.

3. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. Komputery oraz urządzenia, o których mowa wyżej, powinny być zasilane poprzez zastosowanie specjalnych urządzeń podtrzymujących zasilanie. Urządzenia te powinny być wyposażone w oprogramowanie umożliwiające bezpieczne wyłączenie systemu komputerowego. Oznacza to takie wyłączenie, w którym przed zanikiem zasilania zostaną prawidłowo zakończone rozpoczęte transakcje na bazie danych oraz wszelkie inne działania w ramach pracujących aplikacji i oprogramowania systemowego.

4. Dopilnowanie, aby komputery przenośne, w których przetwarzane są dane osobowe, były zabezpieczone hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby mikrokomputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych. Osoby posiadające mikrokomputery przenośne z zapisanymi w nich danymi osobowymi należy przeszkolić w kierunku zachowania szczególnej uwagi podczas ich transportu oraz uczulić na to, aby mikrokomputery te przechowywane były we właściwie zabezpieczonym pomieszczeniu.

5. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe. Dyski i inne informatyczne nośniki danych zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a jeśli nie jest to możliwe, należy uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisu danych osobowych lub naprawiać w obecności osoby upoważnionej przez administratora danych.

6. Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które powinny być zawarte w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

7. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.

8. Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.

9. Nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych.

10. Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

11. Nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny. W zakresie nadzoru, o którym mowa wyżej, administrator bezpieczeństwa informacji powinien dopilnować aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub już niepotrzebnych wydruków komputerowych z danymi osobowymi.

12. 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:

    a) ustalenie identyfikatorów użytkowników i ich haseł (identyfikatory użytkowników należy wpisać do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych),

    b) dopilnowanie, aby hasła użytkowników były zmieniane co najmniej raz na miesiąc,

    c) dopilnowanie, aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,

    d) dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy (również po upływie terminu ich ważności),

    e) dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych, zostały natychmiast wyrejestrowane, a ich hasła unieważnione.

13. Dopilnowanie, aby - jeżeli istnieją odpowiednie możliwości techniczne - ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika. Zalecanym rozwiązanym powyższego problemu jest zastosowanie takich wygaszaczy ekranowych, które po upływie określonego czasu bezczynności użytkownika wygaszają monitor i jednocześnie uruchamiają blokadę, która uniemożliwia kontynuowanie pracy na komputerze bez podania właściwego hasła Wygaszacz taki, oprócz ochrony danych, które przez dłuższy czas byłyby wyświetlane na ekranie monitora, chroniłby system przed przechwyceniem sesji dostępu do danych przez nie uprawnioną osobę.

14. Dopilnowanie, aby w pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych były ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

15. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa wyżej, powinny mieć na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie. W przypadku gdy, na przykład, istnieje podejrzenie, że naruszenie bezpieczeństwa danych osobowych spowodowane zostało zaniedbaniem lub naruszeniem dyscypliny pracy, zadaniem administratora bezpieczeństwa informacji powinno być przedstawienie wniosku administratorowi danych o wszczęcie postępowania wyjaśniającego i ukaranie odpowiedzialnych za to osób.

16. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło), i przygotowanie oraz przedstawienie administratorowi danych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych. Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości. Obowiązek śledzenia skuteczności zabezpieczeń, o którym mowa wyżej, oraz obowiązek ich udoskonalania, nałożony na administratora bezpieczeństwa, wynika bezpośrednio z obowiązku podejmowania odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

WÓJT
Gminy Brody
mgr [illegible]