**PROCEDURA BEZPIECZEŃSTWA FIZYCZNEGO I BEZPIECZEŃSTWA INFORMATYCZNEGO STOWARZYSZENIA**

* 1

Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych stanowią pomieszczenia Stowarzyszenia położone w …

* 2

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności danych przetwarzanych w systemie

1. Środki ochrony fizycznej
* Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami.
* Dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym.
* Nośniki z kopiami zapasowymi zawierających dane osobowe przechowywane są wyłącznie w zamykanych szafach.
1. Środki sprzętowe, informatyczne i telekomunikacyjne
* Stosuje się niszczarki dokumentów.
* Urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania, z wyjątkiem laptopów, które posiadają swoje baterie.
* Sieć lokalna podłączona jest do Internetu poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną.
* Kopie zapasowe wykonywane są raz w tygodniu na nośnikach DVD.
* Automatyczne kopie zapasowe tworzone są na serwerze (dysk D) raz na 24 godziny i przechowane są przez okres 4 dni.
1. Środki ochrony w ramach oprogramowania urządzeń teletransmisji:
* Na komputerach użytkowników systemu działa program antywirusowy.
* Na komputerach użytkowników systemu działa programowy firewall.
* Dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.
1. Środki ochrony w ramach oprogramowania systemu:
* Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników.
* System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika.
* Zastosowano działający w tle program antywirusowy na komputerach użytkowników.
1. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.
* Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
* Dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator.
* Użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.
1. Środki ochrony w ramach systemu użytkowego.
* Komputery, z których możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.
* Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika.
* Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika;
* Komputery, z których możliwy jest dostęp do danych osobowych są szyfrowane.
1. Środki organizacyjne.
* Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone.
* Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez Administratora Danych Osobowych.
* Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.
* Osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym.
* Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
* Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
* Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
* Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy.
* W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą Stowarzyszenia, należy wymontować z niego nośniki informacji zawierające dane osobowe.
* W przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe wymusza konieczność przekazania go poza siedzibę Stowarzyszenia, nośnik ten należy wymontować.
* 4

Procedura postępowania w przypadku naruszenia ochrony danych osobowych

1.Każdy pracownik Stowarzyszenia, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to Administratorowi Danych.

2.W razie braku możliwości zawiadomienia Administratora Danych lub osoby przez niego upoważnionej, należy zawiadomić bezpośredniego przełożonego

3.Do czasu przybycia na miejsce Administratora Danych należy:

* niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony (o ile to możliwe),
* ustalić przyczynę i sprawcę naruszenia ochrony,
* rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
* o ile to możliwe należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia ochrony i udokumentowanie zdarzenia
* podjąć stosowne działania, jeśli zaistniały przypadek został przewidziany w dokumentacji systemu operacyjnego, bazy danych, czy instrukcji aplikacji użytkowej,
* nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych.

4.Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych Administratora Danych podejmuje następujące kroki:

* zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Stowarzyszenia,
* może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
* rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora,
* nawiązuje kontakt ze specjalistami spoza Stowarzyszeniami (jeśli zachodzi taka potrzeba).

5.Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik Nr 4 do polityki ochrony danych osobowych, który zawiera następujące informacje:

* wskazanie osoby zawiadamiającej o naruszeniu, oraz innych osób zaangażowanych w wyjaśnienie okoliczności naruszenia bezpieczeństwa,
* określenie czasu i miejsca zawiadomienia o naruszeniu bezpieczeństwa, jak i samego naruszenia (o ile da się ustalić),
* określenie okoliczności towarzyszących i rodzaju naruszenia,
* opis podjętego działania wraz z wyjaśnieniem wyboru sposobu działania,
* wstępną ocenę przyczyn wystąpienia naruszenia bezpieczeństwa,
* ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego

7.Administrator Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych).

8.Zaistniałe naruszenie bezpieczeństwa może stać się przedmiotem zespołowej analizy przeprowadzanej przez kierownictwo Stowarzyszenia.

9.Analiza ta powinna zawierać wszechstronną ocenę zaistniałego naruszenia bezpieczeństwa, wskazanie odpowiedzialnych, wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencje osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.