Polityka Bezpieczeństwa Danych Osobowych wraz z Instrukcją zarządzania systemem informatycznym przetwarzającym dane osobowe

w POLSKIE TOWARZYSTWO TANECZNE

Wersja 1		**Pieczęć firmowa:**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
DARIUSZ DRAGAN	18.07.2017		.

1. Polityka Bezpieczeństwa

1.1 Wstęp

Polityka Bezpieczeństwa, zwana dalej Polityką, oraz Instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe, zwana dalej Instrukcją, została opracowana zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz wymaganiami określonymi w § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

1.2 Obowiązki Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji

Administratorem Danych Osobowych w myśl Ustawy o ochronie Danych Osobowych jest POLSKIE TOWARZYSTWO TANECZNE.

Do najważniejszych obowiązków ADO, należy:

1. opracowanie i wdrożenie Polityki i Instrukcji (w tym zabezpieczenie zbiorów danych powierzonych do przetwarzania)
2. wydawanie i anulowanie upoważnień dla osób upoważnionych do przetwarzania danych osobowych
3. prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych
4. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
5. nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 UODO, oraz przestrzegania zasad w niej określonych,
6. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

1.3 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Wykaz (fizyczny obszar przetwarzania) ujęto w załączniku **Załącznik B Wykaz_zbiorow_danych_osobowych**

1.4 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych (w tym zbiorów powierzonych do przetwarzania) i programów użytych do przetwarzania tych danych ujęto w **Załączniku B Wykaz_zbiorow_danych_osobowych**

1.5 Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury zbiorów danych osobowych przedstawiono w postaci prostej listy-wykazu pól z danymi osobowymi, odrębnej dla każdego programu służących do przetwarzania danych osobowych – patrz **Załącznik C Opis_struktury_zbiorow_danych**

1.6 Sposób przepływu danych pomiędzy poszczególnymi systemami

Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe przedstawiono w **Załączniku D Sposób przepływu danych pomiędzy poszczególnymi systemami**

1.7 Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1.7.1 Zabezpieczenia organizacyjne

1. **obligatoryjnie:** nie wyznaczono Administratora Bezpieczeństwa Informacji (ABI)
2. **obligatoryjnie:** została opracowana i wdrożona polityka bezpieczeństwa informacji i instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe
3. **obligatoryjnie**: do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych
4. **obligatoryjnie:** prowadzona jest ewidencja osób upoważnionych do przetwarzania danych
5. **obligatoryjnie:** osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego
6. **obligatoryjnie:** osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy
7. o**bligatoryjnie**: przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
8. **obligatoryjnie:** przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych

1.7.2 Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej

1. **obligatoryjnie:** podwójne drzwi zamykane na klucz
2. **obligatoryjnie:** niszczarki dokumentów
3. **obligatoryjnie:** stosuje się sejf

1.7.3 Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. **obligatoryjnie:** zastosowano UPS do serwera lub kluczowych komputerów, na których są przetwarzane dane osobowe
2. **obligatoryjnie:** dostęp do komputera/laptopa zawierającego dane osobowe odbywa się poprzez podanie loginu i hasła
3. **obligatoryjnie:** w przypadku dostępu do danych osobowych przez Internet, stosuje się szyfrowanie tego połączenia (SSL lub VPN)
4. **obligatoryjnie:** w przypadku dostępu do danych osobowych przez Internet, należy uprzednio podać login i hasło
5. **obligatoryjnie:** zastosowano system antywirusowy
6. **obligatoryjnie:** użyto system Firewall do ochrony dostępu do sieci komputerowej
7. **obligatoryjnie:** zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej
8. **obligatoryjnie:** użyto system IDS/IPS do ochrony dostępu do sieci komputerowej

1.7.4 Zabezpieczenia programów przetwarzających dane osobowe

1. **obligatoryjnie:** dla osób upoważnionych do przetwarzania danych osobowych określono zakres przetwarzania (zakres obowiązków)

2. **obligatoryjnie:** dostęp do danych osobowych w systemach/programach informatycznych wymaga podania nazwy użytkownika oraz hasła
3. **obligatoryjnie:** użytkownicy systemów/programów informatycznych posiadają w nich konta z określonymi uprawnieniami
4. **obligatoryjnie:** systemy/programy informatyczne pozwalają na rejestrację kluczowych operacji użytkowników wykonywanych na danych osobowych

2. Instrukcja

2.1 Procedura nadawania uprawnień do przetwarzania danych osobowych.

1. przed nadaniem upoważnienia, osoba jest zapoznana z zasadami ochrony danych osobowych zawartymi w Polityce i Instrukcji
2. osoba zapoznana z zasadami ochrony zobowiązana jest do podpisania Oświadczenia o poufności w **Załączniku E Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych**
3. ADO (lub ABI w imieniu ADO) nadaje upoważnienie osobie upoważnianej wypełniając **Załącznik E Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych Upoważnienie**
4. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie z **Załącznikiem F Ewidencja osób upoważnionych do przetwarzania DO**

2.2 Metody i środki uwierzytelnienia (polityka haseł)

1. hasła nie mogą być powszechnie używanymi słowami
2. użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności i jest zobowiązany jest do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione
3. zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom

2.3 Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. użytkownik loguje się do systemu/programu informatycznego przetwarzającego dane osobowe z użyciem identyfikatora i hasła
2. użytkownik jest zobowiązany do powiadomienia ABI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje
4. użytkownik jest zobowiązany do uniemożliwienia osobom nieupoważnionym (np. stażystom, pracownikom innych działów, pracownikom obcych organizacji) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu
5. przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wylogować się z systemu
6. po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, ewentualnie wyłączyć sprzęt komputerowy oraz stosować politykę czystego biurka dla dokumentów i nośników

2.4. Procedura tworzenia kopii zapasowych

1. procedura obejmuje tworzenie kopii bezpieczeństwa wszystkich programów wraz ze środowiskiem, wymienionych w **Załączniku B_Wykaz_zbiorow_danych_osobowych**

2. kopie całościowe wykonywane są z częstotliwością 7-dniową
3. kopie przyrostowe wykonywane na dedykowanym serwerze backup
4. każda kopia jest czytelnie opisana co do zawartości i daty sporządzenia
5. kopie przechowywane są przez okres 1 roku.
6. dostęp do kopii mają: Informatyk
7. kopie przechowywane są w innym pomieszczeniu niż serwerownia, zabezpieczone w sejfie lub w szafie zamykanej na klucz
8. Informatyk zobowiązany jest do sporządzenia kopii oraz weryfikacji ich poprawności i możliwości ponownego odtworzenia
9. niszczenie kopii odbywa się poprzez trwałe/fizyczne zniszczenie nośnika lub nieodwracalne usunięcie danych z nośnika z użyciem specjalnego oprogramowana

2.5 Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

1. do typowych nośników należą: pen-drive, przenośne twarde dyski, laptopy, dokumentacja papierowa
2. użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników po ustaniu celu ich przetwarzania
3. nośniki są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych)
4. zabrania się wynoszenia poza obszar organizacji niezabezpieczonych nośników z danymi osobowymi bez zgody Administratora Danych Osobowych – nośniki muszą być zaszyfrowane
5. w przypadku wysyłania danych mailem, pliki muszą być zahasłowane a hasło przesłane inną drogą (np. odrębnym mailem)
6. zabrania się przekazywania nośników z nieusuniętymi danymi osobowymi pomiotom lub osobom zewnętrznym (darowizny, naprawy)
7. dane osobowe w postaci papierowej zabezpiecza się co najmniej: w szafach i biurkach zamykanych na klucz
8. zabrania się pozostawiania dokumentów i nośników, jako dostępnych dla osób nieupoważnionych (polityka czystego biurka)
9. niszczenie dokumentów i tymczasowych wydruków musi odbywać się w niszczarkach

2.6 Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

2.6.1 Ochrona antywirusowa

1. każdy z komputerów lub serwer musi być wyposażony w licencjonowany program antywirusowy
2. program antywirusowy musi być aktywny i zabrania się jego wyłączania
3. program antywirusowy musi zawierać aktualną bazę wirusów

2.7 Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. w przypadku udostępnienia danych osobowych innym pomiotom, niż na podstawie wymagań prawa, należy ten fakt odnotować

2. jeżeli system/program informatyczny na to pozwala, dane o udostępnieniu należy wprowadzić do systemu/programu. W przeciwnym wypadku należy dane te wpisać do zaprowadzonej specjalnie w tym celu Ewidencji ręcznej. Ewidencja musi zawierać następujące dane: Data udostępnienia danych, Nazwa i adres podmiotu, któremu dane udostępniono, podstawa prawna udostępnienia danych (Art. 23 / 27 UODO), Zakres udostępnionych danych
3. na żądanie osoby, której dane zostały udostępnione - informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub z Ewidencji ręcznej

2.8. Procedura wykonywania przeglądów i konserwacji

1. zapewniono serwis naprawczy dla sprzętu komputerowego
2. prowadzane są przeglądy i konserwacje systemu informatycznego zgodnie z planem lub wytycznymi producentów
3. naprawa/konserwacja/serwis sprzętu komputerowego i programów, wykonywane przez podmiot zewnętrzny, powinny odbywać się pod ścisłym nadzorem osób upoważnionych
4. przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy trwale usunąć dane osobowe z nośników
5. aktualizację oprogramowania należy przeprowadzać zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki)