POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w

Biurze Rachunkowym T&T A.Tuleja G.Tuleja S.C.
ul. Kochanowskiego 5, 38-200 Jasło

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Biurze Rachunkowym T&T A.Tuleja G.Tuleja S.C., określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych Biura Rachunkowego T&T A.Tuleja G.Tuleja S.C..

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:
1. Ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
2. Danych osobowych - za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. Zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
4. Przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
5. Usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
6. Integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
7. Poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
8. Rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
9. Administratorze Danych Osobowych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydującą o celach i środkach przetwarzania danych osobowych. WBiurze Rachunkowym T&T A.Tuleja G.Tuleja S.C. funkcję tę pełni jeden ze wspólników spółki.
10. Administratorze Bezpieczeństwa Informacji - osoba nadzorująca z upoważnienia Administratora Danych Osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
11. ADO – Administrator Danych Osobowych
12. ABI – Administrator Bezpieczeństwa Informacji
13. Biuro Rachunkowe T&T – skrót od pełnej nazwy Biuro Rachunkowe T&T A.Tuleja G.Tuleja S.C.
14. Placówce – Biuro Rachunkowe T&T A.Tuleja G.Tuleja S.C.
15. Identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

16. Haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
17. Systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
18. Zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem

§ 3

Niniejsza Polityka bezpieczeństwa 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) została opracowana zgodnie z wytycznymi:
1) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietniabv2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunkówbvtechnicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemybvinformatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024),
2) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
Polityka bezpieczeństwa reguluje sprawy ochrony danych osobowych, zawartych w systemach informatycznych oraz w postaci dokumentacji papierowej Biura Rachunkowego T&T. Opisane zasady określają granice zachowania użytkowników systemów informatycznych, wspomagających pracę w Biurze Rachunkowym T&T. Dokument zwraca uwagę na konsekwencje, na jakie mogą się narazić osoby naruszające politykę bezpieczeństwa i nieprzestrzegające jej zasad.
Zabezpieczenia odpowiednie do zagrożeń, ochrona przetwarzanych danych osobowych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi systemom informatycznym. Polityka bezpieczeństwa w Biurze Rachunkowym T&T obowiązuje więc pracowników będących bezpośrednio zatrudnionych przy przetwarzaniu danych osobowych. Dokument ten wskazuje sposób ochrony danych przetwarzanych w sposób tradycyjny oraz środki zabezpieczenia systemów informatycznych, postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy stwierdzono naruszenie zabezpieczeń systemu informatycznego. Wykonywanie postanowień tego dokumentu ma zapewnić odpowiednią reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym w Biura Rachunkowego T&T.

§ 4

Opis zdarzeń naruszających bezpieczeństwo danych osobowych.
Zdarzenia zagrażające bezpieczeństwu danych osobowych podzielono na:
a) zagrożenia zamierzone, świadome i celowe - możliwość naruszenia poufności danych przez nieuprawniony dostęp z zewnątrz lub wewnątrz do systemu informatycznego, przejęcia lub podglądu tych danych przez osoby nieupoważnione,
b) losowe wewnętrzne takie jak: awarie sprzętowe, błędy oprogramowania itd. Istnieje niebezpieczeństwo zniszczenia danych, naruszenia poufności danych,
c) losowe zewnętrzne takie jak: klęski żywiołowe, przerwy w zasilaniu itp.; ich występowanie może prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, nie dochodzi do naruszenia poufności danych.
Główne zdarzenia naruszające bezpieczeństwo danych osobowych lub zakwalifikowane jako uzasadnione podejrzenie naruszenia to:
1) nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu np.: zalanie pomieszczeń, katastrofa budowlana itp.;

2) nadmierna wilgotność, wysoka temperatura i inne czynniki zewnętrzne,
3) awaria sprzętu lub oprogramowania, wyraźnie wskazujące na ingerencję osób trzecich,
4) komunikaty alarmowe systemu lub innego oprogramowania zaangażowanego w proces utrzymywania bezpieczeństwa zbiorów danych,
5) odstępstwa od oczekiwanego działania urządzeń systemu informatycznego wskazujące na możliwe naruszenie bezpieczeństwa danych,
6) naruszenie integralności systemu,
7) naruszenie struktury danych lub nieuprawniona modyfikacja, przejęcie lub podgląd danych osobowych przez osoby nieupoważnione,
8) naruszenie zabezpieczeń pomieszczeń, szaf, biurek i itp., w których przechowywane są zbiory danych w postaci nośników danych lub dokumentacji papierowej.

§ 5

Celem wdrożenia polityki bezpieczeństwa jest ochrona systemu informatycznego jako całości, jego poszczególnych elementów, przetwarzanych przez system zbiorów danych, obszaru, w którym przetwarzane są dane osobowe, a przede wszystkim zapewnienie technicznych i organizacyjnych uwarunkowań mających wpływ na zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe.
Polityka bezpieczeństwa zakłada pełne zaangażowanie dyrekcji oraz pracowników Biura Rachunkowego T&T dla zapewnienia bezpieczeństwa danych osobowych, przetwarzanych w sposób tradycyjny oraz za pomocą systemów informatycznych.
Administratorem Danych Osobowych przetwarzanych w Biurze Rachunkowym T&T jest wspólnik spółki. Dla skutecznej realizacji zasad i reguł polityki bezpieczeństwa Administrator Danych Osobowych zapewnia:
1) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
2) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
3) monitorowanie zastosowanych środków ochrony.
Cele Biura Rachunkowego T&T, w zakresie bezpieczeństwa danych osobowych:
1) ochrona zasobów informacyjnych i zapewnienie ciągłości działania procesów w placówce,
2) zapewnienie zgodności z prawem podejmowanych działań,
3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów Biura Rachunkowego T&T, rozumiane, jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań.

§ 6

Nadrzędną rolą w działaniach Administratora Danych Osobowych, wynikających z jego funkcji, jest ochrona powierzonych danych osobowych. Odpowiedzialność za te dane ponoszą wszyscy pracownicy placówki, mający dostęp do danych osobowych w ramach swoich obowiązków służbowych.
Zarządzanie bezpieczeństwem danych osobowych jest procesem ciągłym, realizowanym przy współdziałaniu osób upoważnionych do przetwarzania danych z Administratorem Danych Osobowych.
Osoby upoważnione do przetwarzania danych osobowych w Biura Rachunkowego T&T zobowiązane są do:
1) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami,
2) postępowania zgodnie z polityką bezpieczeństwa placówki,
3) ścisłego przestrzegania zakresu udzielonego upoważnienia, zachowania w tajemnicy danych osobowych, sposobu ich zabezpieczania oraz zapoznanie się z przepisami dotyczącymi ochrony danych osobowych,
4) natychmiastowego zgłoszenia Administratorowi Danych Osobowych lub Administratorowi Bezpieczeństwa Informacji podejrzenia lub stwierdzenia faktu naruszenia bezpieczeństwa danych

osobowych przetwarzanych w szkole.

§ 7

1. ADO zobowiązany jest do zapewnienia, aby dane osobowe były:
1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych celów, zgodnych z prawem,
3) merytorycznie poprawne i adekwatne w stosunku do celów.
2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
5. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. Organizuje szkolenia mające na celu zapoznanie każdej osoby, przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. Odpowiada za to, by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:
1) ochronę danych przed niepowołanym dostępem,
2) nieuzasadnioną modyfikację lub zniszczenie danych,
3) nielegalne ujawnienie danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

§ 8

Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
1) ochrony danych osobowych, zawartych w zbiorach systemów informatycznych szkoły,
2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa”, w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
3) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nich zatrudnionych.

§ 9

Obowiązki Administratora Bezpieczeństwa Informacji (ABI):
1. Nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.
2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
3. Nadzór na wykorzystywanym w Biurze Rachunkowym T&T oprogramowaniem oraz jego legalnością.
4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe.
5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.
6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.

7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
8. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
9. Definiowanie użytkowników i haseł dostępu.
10. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.
11. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
12. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
13. Prowadzenie ewidencji osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 6.
14. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego

§ 10

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe zawiera załącznik nr 2 do Polityki bezpieczeństwa.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych zawiera załącznik nr 3 do Polityki bezpieczeństwa.
3. Opis struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych, zawiera załącznik nr 4 do Polityki bezpieczeństwa.
4. Upoważnienie do przetwarzania danych osobowych zawiera załącznik nr 5.
5. Ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych w podmiocie, zawiera załącznik nr 6
6. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, zawiera załącznik nr 7.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w

Biurze Rachunkowym T&T A.Tuleja G.Tuleja S.C.
ul. Kochanowskiego 5, 38-200 Jasło

§ 1

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 poz. 1182 z późn. zm.), Rozporządzenie 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. z 2004 r. Nr 100, poz. 1024) nakłada na Administratora

Danych Osobowych następujące obowiązki:
1) zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
2) zabezpieczenie danych przed nieuprawnionym dostępem,
3) zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
4) zabezpieczenie przed utratą danych,
5) zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.
Ochronie podlegają dane osobowe, niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.
Zawarte w instrukcji procedury i wytyczne są przekazywane osobom odpowiedzialnym za ich realizację stosownie do przyznanych uprawnień i zakresu obowiązków. Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i system informatyczny, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

§ 2

1. Celem instrukcji jest określenie sposobu zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.
2. Instrukcja Zarządzania Systemem Informatycznym, służącym do przetwarzania danych osobowych w Biurze Rachunkowym T&T, zwaną dalej instrukcją - określa sposób zarządzania oraz zasady administrowania systemem informatycznym, służącym do przetwarzania danych osobowych.

Ilekroć w instrukcji jest mowa o:
1) placówce - rozumie się przez to Biuro Rachunkowe T&T A.Tuleja G.Tuleja S.C.
2) kierowniku jednostki - rozumie się przez to wsplnikw spółki,
3) danych osobowych - rozumie się przez to każdą informację, dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby,
4) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,
5) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych

osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
6) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
7) Administratorze Danych Osobowych (ADO) - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w wypadku naruszeń w systemie zabezpieczeń. Funkcję ADO pełni jeden ze wspólników spółki,
8) Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę nadzorującą, (upoważnioną przez ADO), przestrzeganie stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzania danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
9) Administratorze Sieci/Systemu Operacyjnego - rozumie się przez to osobę nadzorującą i odpowiadającą za poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego w danej jednostce organizacyjnej, w tym w szczególności:
a) mającą prawo do zmiany uprawnień wszystkich użytkowników,
b) za pomocą platformy zarządzania, dysponującą bezpośrednio wszystkimi zasobami podległej mu sieci,
c) pełniącą kontrolę nad dostępem użytkowników do systemów,
d) podejmującą samodzielnie lub na polecenie Administratora Bezpieczeństwa Informacji odpowiednie działania w wypadku naruszeń w systemie zabezpieczeń
e) funkcję tą pełni dyrektor jeden ze wspólników spółki.
9. Administratorze Aplikacji - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo przetwarzania danych w ramach aplikacji, w tym administrującą prawami dostępu w ramach eksploatowanych aplikacji,
10. użytkownikach systemu - rozumie się osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym,
11. obszarze kontrolowanym – rozumie się przez to obszar znajdujący się pod ochroną, o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych, w tym danych osobowych.

§ 3

Niniejsza Instrukcja Zarządzania Systemem Informatycznym określa:
1) poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym,
2) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym,
3) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
4) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
5) procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu;
6) metodę i częstotliwość tworzenia kopii awaryjnych.
7) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
8) sposób, miejsce i okres przechowywania:
a) elektronicznych nośników informacji zawierających dane osobowe;
b) kopii zapasowych,
9) sposobu dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
10)sposobu postępowania w zakresie komunikacji w sieci komputerowej,
11)procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących

do przetwarzania danych.

§ 4

Zasady nadawania i rejestrowania uprawnień do przetwarzania danych osobowych wraz ze wskazaniem osób odpowiedzialnych w tym zakresie jeden ze wspólników Biura Rachunkowego T&T upoważnia pracowników do przetwarzania danych osobowych do niniejszej instrukcji. Upoważnienia do przetwarzania danych osobowych przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja. Ewidencje prowadzą kadry placówki.

§ 5

Stosowane metody i środki uwierzytelnienia:

1) W systemach oraz programach komputerowych służących do przetwarzania danych osobowych stosowane jest uwierzytelnianie pracownika przy pomocy jego identyfikatora i hasła.
2) Pracownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami.
3) Identyfikator pracownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
4) Hasło użytkownika bazy danej składa się z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
5) Pracownik jest zobowiązany zmienić hasło, o ile system na to pozwala, co najmniej raz na 60 dni.
6) Każdy pracownik zarządza swoimi hasłami.
7) Hasło pracownika jest jego własnością i zna je wyłącznie dany pracownik oraz wspólnicy Biura Rachunkowego T&T.
8) Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych pracowników. Jeżeli pracownik w pobliżu zaczyna wprowadzać hasło należy odwrócić wzrok.

§ 6

Zasady korzystania z systemu przez użytkowników (rozpoczęcia, zawieszenia i zakończenia pracy):

1) Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).
2) Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji.
3) Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.
4) Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają uprawnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane. Krzesło interesanta ustawione jest w taki sposób, by nie mógł patrzeć na ekran monitora.
5) Pomieszczenia, w których przetwarzane są dane osobowe należy zamykać na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.

§ 7

Środki stosowane do zabezpieczenia systemu informatycznego:

1) Na wszystkich stacjach roboczych oraz serwerach zainstalowane jest oprogramowanie antywirusowe.
2) Elektroniczne nośniki informacji należy każdorazowo sprawdzić programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie.
3) W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z ADO.

4) Zabrania się użytkownikom komputerów wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem. Wszyscy pracownicy poinformowani są o zakazie instalowania nielegalnego oprogramowania.

§ 8

Udostępnianie danych osobowych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek, zgodnie z przepisami prawa.

§ 9

Zasady dokonywania przeglądów i konserwacji systemów oraz nośników informacji:
1) Przeglądy i konserwacje systemów oraz zbiorów danych wykonuje ADO na bieżąco.
2) Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt w miejscu jego użytkowania.
3) W przypadku konieczności naprawy poza miejscem użytkowania sprzęt komputerowy przed oddaniem do serwisu powinien być odpowiednio przygotowany. Dane należy archiwizować na nośniki informacji, a dyski twarde wymontowywać na czas naprawy.