Polityka Bezpieczeństwa w zakresie przetwarzania danych osobowych w Zakładzie Budownictwa Liniowego Telbial Sp. z o. o

Polityka Bezpieczeństwa, zwana dalej Polityką, oraz Instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe, zwana dalej Instrukcją, została opracowana w celu wykazania, że dane osobowe są przetwarzane zgonie z wymogami prawa dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000), wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywny 95/46/WE (zwanego dalej RODO) 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).

Definicje:

- **Administrator Danych** – Zakład Budownictwa Liniowego TELBIAL sp. zo.o.
- **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba to osoba fizyczna, która można pośrednio lub bezpośrednio zidentyfikować na podstawie identyfikatora takiego jak imię i nazwisko, numer indentyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jednej bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych , takie jak· zbieranie , utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych
- **Użytkownik** – każda osoba upoważniona przez Administratora danych do przetwarzania danych osobowych
- **Zbiór danych-** każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określnych kryteriów

I. INFORMACJE DOTYCZĄCE DANYCH

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.

2. Administrator Danych nie podejmuje czynności przetwarzania, które mogłyby wiązać z prawdopodobieństwem wystąpienia ryzyka dla praw i wolności osób, zaś w przypadku planowania takich działam Administrator podejmie czynności określone w art. 35 i następne RODO.
3. W zakresie nowych czynności przetwarzania Administrator Danych zobowiązuje się uwzględnić kwestie ochrony danych już na etapie ich planowania.

1. Obowiązki Administratora Danych Osobowych

Do najważniejszych obowiązków ADO, należy:

a) opracowanie i wdrożenie Polityki i Instrukcji (w tym zabezpieczenie zbiorów danych powierzonych do przetwarzania)
b) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych i RODO
c) zapewnienie przetwarzania danych zgodnie z uregulowaniami polityki bezpieczeństwa informacji oraz w zakresie jakim jest to niezbędne do osiągnięcia celu przetwarzania danych
d) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
e) nadzór nad bezpieczeństwem danych osobowych,
f) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
g) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;

Administrator Bezpieczeństwa Informacji ma prawo :

a) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji
b) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
c) żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
d) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
e) żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych

2. **Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe**

a) Jest to tak zwany Obszar przetwarzania danych osobowych. Wykaz ujęto w Załączniku 1

3. **Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych**

a) Wykaz zbiorów danych osobowych (w tym zbiorów powierzonych do przetwarzania) i programów użytych do przetwarzania tych danych ujęto w Załączniku 2

4. **Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych**

a) Zabezpieczenia organizacyjne

- obligatoryjnie: została opracowana i wdrożona polityka i instrukcja

- obligatoryjnie: osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych, przepisów RODO oraz w zakresie zabezpieczeń systemu informatycznego

- obligatoryjnie: każdy z przetwarzających dane osobowe jest pisemnie upoważniony do ich przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" stanowiącym załącznik nr 4 do niniejszej Polityki Bezpieczeństwa

- obligatoryjnie: osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy zgodnie z „Oświadczeniem o zachowaniu w tajemnicy przetwarzania danych osobowych" stanowiącym załącznik nr 5 do Polityki Bezpieczeństwa

- -obligatoryjnie: przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych

- 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

- obligatoryjnie: Pracownicy zobowiązani są do:

- ✓ Ścisłego przestrzegania zakresu nadanego upoważnienia (stanowiącego załącznik nr 1 do niniejszej Polityki)
- ✓ Przetwarzania i ochronnych danych zgodnie z przepisami RODO i ustawy o ochronie danych osobowych
- ✓ Zachowania w tajemnicy danych osobowych (zgodnie z załącznikiem nr 2 do Polityki Bezpieczeństwa) ;
- ✓ Zgłaszania wszelkich incydentów dotyczących naruszenia bezpieczeństwa danych.

b) Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektroniczne

- główne drzwi do budynku zabezpieczone alarmem

- obligatoryjnie: drzwi zamykane na klucz

- obligatoryjnie: zamknięte niemetalowe szafy

- obligatoryjnie: niszczarki dokumentów

- obligatoryjnie: stosuje się politykę kluczy

c) Polityka kluczy:

- dostęp do budynków i pomieszczeń biurowych możliwy jest wyłącznie przez osoby upoważnione na mocy „Upoważnienia do przetwarzania danych osobowych" stanowiącego załącznik nr 1 do niniejszej Polityki Bezpieczeństwa, które posiadają do nich klucze

- klucze poza godzinami pracy osoby upoważnione sprawują nad nimi całodobowy nadzór osobisty

- klucze zapasowe przechowywane są w wyznaczonych i zabezpieczonych miejscach

- wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą bezpośredniego przełożonego.

- klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu

- w godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie

- zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu

- po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu

- naruszenie zasad polityki kluczy może spowodować wyciągnięcie następujących konsekwencji: Poniesienie odpowiedzialności wynikających z art. 52 kodeksu pracy lub poniesienie odpowiedzialności wynikających z art. 363 §1. kodeksu cywilnego.

d) System alarmowy przeciwwłamaniowy

e) System przeciwpożarowy /gaśnice

5. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

a) obligatoryjnie: zastosowano UPS do serwera lub kluczowych komputerów, na których są przetwarzane dane osobowe
b) obligatoryjnie: zastosowano system antywirusowy
c) obligatoryjnie: użyto system Firewall do ochrony dostępu do sieci komputerowej
d) obligatoryjnie - zabezpieczenie dostępu do urządzeń Administratora Danych przy pomocy haseł dostępu
e) wykorzystywanie szyfrowania danych przy ich transmisji

6. Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą Administratora danych osobowych i za wiedzą Administratora bezpieczeństwa informacji. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony pracownika za wiedzą administratora bezpieczeństwa informacji.

Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. Użytkownik komputera przenośnego zobowiązany jest do:

- ✓ transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
- ✓ o transportowania komputera w bagażu podręcznym, o nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp, o zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych.
- ✓ korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
- ✓ nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
- ✓ zabezpieczania komputera przenośnego hasłem,
- ✓ blokowanie dostępu do komputera przenośnego w przypadku gdy nie jest on wykorzystywany przez pracownika,
- ✓ kopiowanie danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,
- ✓ umożliwienia, poprzez podłączenie komputera do sieci informatycznej OPI aktualizacji wzorców wirusów w programie antywirusowym,
- ✓ utrzymanie konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,
- ✓ wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
- ✓ zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

Administrator bezpieczeństwa informacji zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:

- ✓ dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości

Administrator bezpieczeństwa informacji jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych, w szczególności ewidencja obejmuje:

- ✓ typ i numer seryjny komputera przenośnego,
- ✓ imię i nazwisko osoby będącej użytkownikiem komputera, •
- ✓ oprogramowanie zainstalowane na komputerze,

- ✓ rodzaj i zakres danych osobowych przetwarzanych na komputerze przenośnym.

W razie zgubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia administratora bezpieczeństwa informacji lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

7. Zabezpieczenia programów przetwarzających dane osobowe

a) obligatoryjnie: dla osób upoważnionych określono zakres obowiązków i prawa dostępu do danych osobowych
b) obligatoryjnie: dostęp do danych osobowych w systemach/programach informatycznych wymaga podania nazwy użytkownika oraz hasła
c) opcjonalnie: użytkownicy systemów/programów informatycznych posiadają w nich konta z określonymi prawami dostępu
d) opcjonalnie: zmianę haseł wymusza system

8. Naruszenie zasad ochrony danych osobowych

a) w przypadku naruszenia danych osobowych Administrator Danych zobowiązuje się dokonać oceny ryzyka naruszenia praw i wolności osób fizycznych

b) w przypadku kiedy zaistniałej naruszenie danych osobowych mogło spowodować ryzyko naruszenia praw i wolności osób fizycznych Administrator Danych zgłasza fakt tego naruszenia organowi nadzorczemu w sposób niezwłoczny nie później niż w terminie 72 godzin od naruszenia zgodnie z „Zgłoszeniem incydentu naruszenia danych osobowych" stanowiącym załącznik nr 7 do Polityki Bezpieczeństwa

c) jeżeli ryzyko naruszenia praw i wolności jest wysokie Administrator zawiadamia o incydencie osobę, której naruszenia dotyczy

9. Postanowienia końcowe

a) kierownicy komórek organizacyjnych są obowiązani zapoznać z treści Polityki każdego użytkownika
b) użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych i RODO, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką bezpieczeństwa
c) w sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych i RODO oraz wydanych na jej podstawie aktów wykonawczych.

d) użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce i w tym zakresie podpisują oświadczenie o zaznajomieniu z Polityką Bezpieczeństwa i przepisami prawa według wzoru stanowiącego Załącznik nr 6 do niniejszej Polityki.

10. Lista załączników

a) Załącznik nr 1 - wykaz pomieszczeń, w których przetwarzane są dane osobowe.
b) Załącznik nr 2 - wykaz zbiorów danych osobowych oraz programy zastosowane do ich przetwarzania.
c) Załącznik nr 3 - Lista osób, które zapoznały się z „Polityką bezpieczeństwa w zakresie ochrony danych osobowych w Zakładzie Budownictwa Liniowego Telbial Sp. z o. o."
d) Załącznik nr 4 – Upoważnieniem do przetwarzania danych osobowych
e) Załącznik nr 5 - Oświadczenie o zachowaniu w tajemnicy przetwarzania danych osobowych
f) Załącznik nr 6 – Oświadczenie o zaznajomieniu z Polityką Bezpieczeństwa i przepisami prawa.
g) Załącznik nr 7 - Zgłoszenie incydentu naruszenia danych osobowych
h) Załącznik nr 8 - Lista wymaganych środków technicznych i organizacyjnych/koncepcja bezpieczeństwa

Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

1. Adres budynku:
   ul. Brzeska 134, 21-500 Biała Podlaska

   Wykaz pomieszczeń:
   - Gabinet Dyrektora
   - Sekretariat i Księgowość
   - Biuro Projektu „Internet nowej generacji dla ziemi terespolskiej."
   - Serwerownia (kontener telekomunikacyjny przy ul. Narutowicza w Białej Podlaskiej)

2. Adres budynku:
   ul. Wojska Polskiego 134, 21-550 Terespol

   Wykaz pomieszczeń:
   - Biuro Obsługi Klienta

Wykaz zbiorów danych osobowych oraz programy zastosowane do ich przetwarzania.

Zbiory danych osobowych:

1. Dane osobowe dotyczące firm oraz instytucji
2. Dane osobowe klientów indywidualnych

Programy do przetwarzania danych osobowych:

1. Program Kadrowo – Płacowy WF Gang
2. System sprzedaży Subiekt GT
3. System finansowo księgowy Rewizor GT
4. Oprogramowanie LMS

Lista osób, które zapoznały się z „Polityką bezpieczeństwa w zakresie ochrony danych osobowych w Zakładzie Budownictwa Liniowego Telbial Sp. z o. o."

L.p.	Imię i nazwisko	Data	Podpis
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

14			
15			
16			
17			
18			
19			
20			
21			

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),**
niniejszym upoważniam do przetwarzania danych osobowych:
_____ *(imię, nazwisko)* zatrudnionego/nej na podstawie
umowy o pracę z dnia ..... na stanowisku _____
w celach i zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.
Upoważniam _____ *(imię i nazwisko)* do przetwarzania danych osobowych zawartych w następujących zbiorach: rejestry, ewidencje, spisy itp. oraz prowadzonych w formie elektronicznej
Upoważnienie obejmuje uprawnienie do przetwarzania danych w zakresie (*w tym miejscu należy wskazać kategorie danych oraz operacje na danych osobowych, jakich może dokonywać upoważniony do przetwarzania danych osobowych)*:

- Dane klientów oraz potencjalnych klientów ZBL Telbial Sp. z o. o. (korespondencja, kontakt bezpośredni).
- Dane kontrahentów i podmiotów współpracujących (korespondencja, kontakt bezpośredni).

Okres ważności upoważnienia: .....
Niniejsze umocowanie upoważnia tylko do czynności wyraźnie w nim wskazanych i nie stanowi wyznaczenia do dokonywania w imieniu pracodawcy czynności z zakresu prawa w rozumieniu art. 3^1 Kodeksu Pracy.

....

(miejscowość i data) *(czytelny podpis)*

Biała Podlaska, dnia.....

.....

(imię i nazwisko pracownika)

.....

(stanowisko)

OŚWIADCZENIE O ZACHOWANIU W TAJEMNICY PRZETWARZANIA DANYCH OSOBOWYCH

W związku z udzielonym mi w dniu ..... upoważnieniem do przetwarzania danych osobowych, niniejszym zobowiązuje się do:

1. zachowania w tajemnicy wszelkich danych osobowych, do których mam dostęp w związku z wykonywaniem zadań służbowych zarówno w trakcie trwania stosunku pracy jak i po jego ustaniu;
2. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, do których mam dostęp w związku z wykonywaniem zadań służbowych.
3. Chronić dane osobowe przed dostępem osób do tego nieupoważnionych

Powyższej tajemnicy zobowiązuje się dochować również po ustaniu zatrudnienia.

....

(miejscowość i data) *(czytelny podpis)*

Biała Podlaska, dnia .....

.....

(imię i nazwisko pracownika)

.....

(stanowisko)

OŚWIADCZENIE O ZAZNAJOMIENIU Z PRZEPISAMI POLITYKI BEZPIECZEŃSWTA i PRZEPISAMI PRAWA

W związku z udzielonym mi w dniu ..... upoważnieniem do przetwarzania danych osobowych, niniejszym oświadczam, że:

— zostałem zaznajomiony z Polityką Bezpieczeństwa obowiązującą w Zakładzie Budownictwa Liniowego TELBIAL sp. z o.o. oraz przepisami ustawy o ochronie danych osobowych i RODO

— zobowiązuję się do bezwzględnego przestrzegania postanowień Polityki Bezpieczeństwa

....

(miejscowość i data) *(czytelny podpis)*

.....dnia.....

Prezes Urzędu Ochrony Danych Osobowych

ul. Stawki 2, 00-193 Warszawa
LUB
przez elektroniczną skrzynkę podawczą
dostępną na stronie:
https://www.uodo.gov.pl/pl/p/kontakt

ZGŁOSZENIE INCYDENTU NARUSZENIA DANYCH OSOBOWYCH

Działając na podstawie art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych

Dane Administratora Danych Osobowych	Zakład Budownictwa Liniowego TELBIAL sp. z o.o. , ul. Brzeska 134; 21-500 Biała Podlaska
Data i miejsce naruszenia	
Kategoria i liczba osób której dane dotyczą	
Opis charakteru naruszenia ochrony danych	
Środki zastosowane w celu wyeliminowania naruszenia danych	

....

(miejscowość i data) *(podpis osoby uprawionej do reprezentowania Administratora Danych)*

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją Zarządzania" wprowadza się w oparciu o wymogi bezpieczeństwa informacji określone w rozporządzeniu 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). System, na którym pracują użytkownicy, jest zbiorem samodzielnych lub połączonych zależnościami podsystemów informatycznych w których ma miejsce przetwarzanie danych osobowych.

I

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§1

1. Użytkownikowi zostaje przyznany unikalny w konkretnym podsystemie identyfikator wraz z poufnym hasłem.
2. O przyznaniu identyfikatora decyduje Administrator Danych, co jest tożsame z przyznaniem użytkownikowi prawa do przetwarzania danych osobowych w systemie informatycznym.
3. Identyfikator wraz z prawidłowym hasłem umożliwia użytkownikowi dostęp do podsystemu przetwarzania danych osobowych.

4. Każdy z użytkowników przed dopuszczeniem do podsystemu podpisuje umowę o zachowaniu poufności (Załącznik nr 5 do Polityki Bezpieczeństwa), zapoznaje się z Instrukcją Zarządzania i Polityką Bezpieczeństwa oraz zostaje pouczony o wdrożonych procedurach bezpieczeństwa.
5. Administratorowi Bezpieczeństwa Informacji przysługuje prawo do zablokowania konta użytkownika w każdym czasie.
6. Po zakończeniu operacji w systemie informatycznym, użytkownik zobowiązany jest wylogować się z podsystemu.
7. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych – każdy użytkownik zobowiązany jest do niezwłocznego powiadomienia Administratora Danych lub Administratora Bezpieczeństwa Informacji.
8. Użytkownikom przyznaje się równe uprawnienia w dostępie do podsystemu (poziom podstawowy) chyba, że specyfika systemu wymaga innego podejścia.
9. Administratorowi Bezpieczeństwa Informacji przysługuje prawo dostępu do podsystemu na poziomie wyższym (Administratora Systemu).

II

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§2

1. Użytkownicy którym przyznano dostęp do podsystemu przetwarzania danych osobowych (w tym identyfikator dostępu do systemu) ustalają hasło dostępu z Administratorem Bezpieczeństwa Informacji.

2. Hasło jest informacją o poufnym charakterze i należy zachować je w tajemnicy.

3. Obowiązuje ścisły zakaz ujawniania hasła osobom trzecim, w tym innym użytkownikom.

§3

1. Hasło składa się z ciągu co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasła są różne dla każdego z użytkowników.

3. Hasła są przechowywane w podsystemie w postaci zaszyfrowanej.

4. Para „identyfikator i hasło" przyznane jednemu użytkownikowi nie może zostać powtórnie wykorzystane.

5. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej.

III

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§4

1. W celu uruchomienia podsystemu informatycznego użytkownik powinien:

a) uruchomić komputer,
b) wybrać odpowiednią opcję umożliwiającą logowanie do podsystemu,
c) zalogować się do podsystemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.

2. Użytkownik podczas logowania do podsystemu nie może ujawniać hasła osobom trzecim, w tym innym administratorom oraz pozostawiać zapisanego hasła w pobliżu stanowiska pracy i innych pracowników.

3. Użytkownik zobligowany jest do skutecznego wylogowania się z podsystemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego na jak długo ma zamiar odejść od komputera.

4. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.

5. Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych.

6. W przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu, użytkownik niezwłocznie zawiadamia o zaistniałym fakcie Administratora Bezpieczeństwa Informacji.

IV

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§5

1. Kopie zapasowe zbiorów danych osobowych tworzone są na bieżąco po zakończonym dniu pracy ze zbiorem

2. Kopie zapasowe tworzone są automatycznie i zapisywane są na zapasowym nośniku danych.

3. Poprawność procesu tworzenia i przechowywania kopii zapasowych – nadzoruje Administrator Bezpieczeństwa Informacji.

V

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§6

1. Elektroniczne nośniki informacji zawierające dane osobowe są przechowywane
w zamkniętych szafkach z zabezpieczeniem dostępu osób trzecich.

2. Kopie są niezwłocznie zniszczone po ustaniu użyteczności danych osobowych tam zawartych.

3. Zniszczenia kopii dokonuje się w sposób uniemożliwiający późniejsze odtworzenie danych, poprzez fizyczne zniszczenie nośników danych lub jeśli to niemożliwe, poprzez trwałe usunięcie danych przy pomocy specjalistycznego oprogramowania służącego do tego celu. W przypadku wątpliwości, należy zwrócić się do Administratora Bezpieczeństwa Informacji.

4. Kopie zapasowe przechowuje się przez okres 2 lat o ile przepisy nie stanowią inaczej, lub gdy użyteczność danych osobowych ustała przed upływem 2 lat licząc od dnia utworzenia kopii zapasowej, na której te dane są utrwalone.

VI

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do 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)

§7

1. System informatyczny Instytutu jest zabezpieczony przed atakami z zewnątrz sieci za pomocą oprogramowania typu firewall. Dodatkowo na serwerze pocztowym program antywirusowy chroni system przed przedostaniem się do wewnątrz sieci złośliwego oprogramowania.

2. Komponenty serwerowe chronione są przed zakłóceniami w sieci zasilającej przy pomocy urządzeń typu UPS, podtrzymujących zasilanie.

3. Każdy podsystem w którym ma miejsce przetwarzanie danych osobowych, podlega ochronie przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym aktualizowanym na bieżąco.

4. W celu przeciwdziałania atakom zainfekowanych plików, podsystem musi być skanowany pod kątem obecności w systemie wirusów i innych zagrożeń.

5. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadamia Administratora Bezpieczeństwa Informacji.

6. Wszystkie komputery, na których uruchomione są podsystemy przetwarzające dane osobowe muszą być zaopatrzone w urządzenia typu UPS, podtrzymujące zasilanie, a tym samym zabezpieczające podsystem przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

7. W przypadku stwierdzenia braku zasilania należy dokonać natychmiastowego zapisu danych osobowych oraz przeprowadzić procedurę opuszczenia podsystemu.

VII

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§8

1. Przeglądów oraz konserwacji systemu dokonuje Administrator Bezpieczeństwa Informacji.

2. W przypadku przekazania innym podmiotom elementów systemu w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte. Proces ten nadzoruje Administrator Bezpieczeństwa Informacji.

3. Dane osobowe muszą być zabezpieczone przed dostępem osób trzecich zanim nośnik lub element systemu zostanie przekazany podmiotowi innemu niż Administrator Informacji lub Administrator Bezpieczeństwa Informacji.

VIII

Uwagi końcowe

§10

1. Dopuszcza się możliwość wprowadzania w Instrukcji Zarządzania procedur uzupełniających, jeśli wymagać będzie tego specyfika komórki organizacyjnej.

2. Tekst Instrukcji Zarządzania jest udostępniany użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia.