# INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

WEGA-MIKOŁÓW Sp. z.o.o. Sp. Kom.
NIP: 6351832321, REGON: 243342092

……
*(nazwa podmiotu)*

ul. Przyjaciół 125, 43-190 Mikołów

……
*(siedziba: adres pocztowy)*

## ROZDZIAŁ 1
### Postanowienia ogólne

**§ 1**

Stosownie do postanowień § 3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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), niniejszym ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych **zwaną dalej Instrukcją Zarządzania Systemem Informatycznym.**

**§ 2**

Instrukcja ma zastosowanie na obszarze wskazanym w Polityce Bezpieczeństwa przetwarzania danych osobowych, w którym przetwarzane są dane osobowe w systemie informatycznym.

**§ 3**

Ilekroć w Instrukcji jest mowa o:

- **systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
- **zabezpieczeniu systemu informatycznego** – należy przez to rozumieć zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz
  kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem.
- **zbiorze danych osobowych** – 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;

- **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;
- **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
- **Administratorze Danych Osobowych –** rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych,
- **administratorze Bezpieczeństwa Informacji –** rozumie się przez to osobę wyznaczoną przez Administratora danych osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- **Administratorze Systemu Informatycznego -** rozumie się przez to osobę wyznaczoną przez administratora danych, nadzorującą przestrzeganie i zabezpieczenie zasad ochrony danych osobowych przez użytkowników systemów informatycznych,
- **użytkowniku** – rozumie się przez to upoważnionego przez administratora danych (w przypadku powołania Administratora Bezpieczeństwa Informacji również przez ABI), wyznaczonego do przetwarzania danych osobowych pracownika;
- **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
- **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
- **nośniki danych osobowych** – dyskietki, laptopy, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi.

**§ 4**

Ogólną kontrolę i nadzór nad przestrzeganiem postanowień niniejszej Instrukcji sprawuje powołany Adminstrator Systemów Informatycznych, powołanie ASI stanowi **załącznik nr 1** do Instrukcji Zarządzania Systemem Informatycznym
a w szczególności realizuje poniższe zadania:

- sam lub za pomocą wyznaczonej przez siebie osoby sporządza kopie bezpieczeństwa dla baz sieciowych;
- pozbawia urządzenia i inne nośniki informacji przeznaczone do likwidacji zapisu danych lub – gdy nie jest to możliwe – uszkadza je trwale w sposób uniemożliwiający odczytanie danych;
- nadzoruje usuwanie awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych;
- zabezpiecza zbiory danych osobowych wysyłanych poza obszar określony w Polityce Bezpieczeństwa;
- sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe;
- sam lub za pomocą wyznaczonej osoby sprawuje nadzór nad czynnościami związanymi z ochroną przeciwwirusową, czynnościami serwisowymi dotyczącymi systemu informatycznego, w którym przetwarzane są dane osobowe;
- nadzoruje obieg i przetwarzanie wydruków z systemu informatycznego zawierających dane

osobowe;
- podejmuje i nadzoruje wszelkie inne działania zmierzające do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.

# ROZDZIAŁ 2
## Zakres przedmiotowy Instrukcji

**§ 1**

.
Niniejsza Instrukcja zawiera w szczególności:
- sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazania osób odpowiedzialnych za te czynności,
- sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazania osób odpowiedzialnych za te czynności,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy,
- metody i częstotliwość tworzenia kopii awaryjnych,
- metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
- sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
- sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
- sposób postępowania w zakresie komunikacji w sieci komputerowej.

**§ 2**

Działaniem Instrukcji objęci są:
- Administrator Danych Osobowych,
- Administrator Bezpieczeństwa Informacji *(o ile został powołany),*
- Administrator Systemu Informatycznego ( *o ile został powołany*),
- osoby zatrudnione przy przetwarzaniu danych osobowych,
- osoby, które przetwarzają dane osobowe w systemach informatycznych.

**§ 3**

Wykaz urządzeń służących do przetwarzania danych stanowi **załącznik nr 2** do niniejszej Instrukcji.

# ROZDZIAŁ 3
## Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

**§ 1**

- Osobą odpowiedzialną za nadawanie uprawnień do przetwarzania danych w systemach informatycznych jest Administrator Systemów Informatycznych
- Wzór wniosku o nadanie/zmianę/cofnięcie uprawnień składanego przez Kierowników poszczególnych działów stanowi **załącznik nr 3** do niniejszej Instrukcji;
- Użytkownikiem systemu informatycznego może być jedynie osoba posiadająca odpowiednie

upoważnienie i zarejestrowana w rejestrze użytkowników;
- Rejestr użytkowników systemu, stanowiący **załącznik nr 4** do niniejszej Instrukcji i prowadzi ją Administrator Systemów Informatycznych;
- Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego identyfikatorem i hasłem dostępu;

Nadawanie identyfikatorów i przydzielanie haseł
- w celu jednoznacznego określenia użytkowników przyjmuje się następującą metodologię nadawania nazw kont: pierwsza litera i cztery pierwsze litery nazwiska
- hasło powinno składać się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne,
- zmiana hasła powinna być wymuszana przez system i wykonywana co 30 dni,
- identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie,
- identyfikatory użytkowników ujawnione są w wykazie osób upoważnionych do przetwarzaniu danych osobowych,
- hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie, obowiązek ten rozciąga się także na okres po upływie ważności hasła,
- hasło, co do którego zaistniało choćby podejrzenie ujawnienia powinno być niezwłocznie zmienione przez użytkownika,
- utrata upoważnienia do przetwarzania danych osobowych, powoduje natychmiastowe usunięcie z grona użytkowników systemu informatycznego.

**§ 2**

Indywidualny zakres czynności osoby upoważnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed:
- niepowołanym dostępem,
- nieuzasadnioną modyfikacją lub zniszczeniem,
- nielegalnym ujawnieniem,
- pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
- jeżeli istnieje taka możliwość, ekrany monitorów, na których możliwy jest dostęp do danych osobowych, powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
- monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

# ROZDZIAŁ 4

## Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

**§ 1**

Zabezpieczenia odnoszą się do:
- technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania:
  - zastosowano zasilanie awaryjne UPS, listwy przepięciowe,

a. komputery służące do przetwarzania danych osobowych są połączone z lokalną siecią

publiczną i posiadają zabezpieczonie firewall,

b. programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje,

c. ograniczono dostęp do sieci lokalnej - zablokowano portale społecznościowe oraz dostęp do poczty prywatnej pracowników,

- sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji,

a. lokalizacja urządzeń komputerowych (komputerów typu PC, drukarek) uniemożliwia osobom niepowołanym (np. petentom,klientom, osobom nieuprawnionym) dostęp do nich.

b. dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem: identyfikatora i hasła

c. dostęp do dysków tylko z uprawnieniami administratora systemów

- sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji),

a. dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.

**Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym**

- Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
- zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym – hasło nie może zawierać mniej niż 8 znaków,
- osoba je tworząca obowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.,
- sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
- w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego oraz osobę nadzorująca przypadki naruszeń,
- w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.
- Przerywając przetwarzanie danych użytkownik powinien co najmniej: aktywować wygaszasz ekranu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby.
  Zalecane jest w takich przypadkach: skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem (hasło powinno być zbieżne z hasłem logowania do systemu),
- zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.
- Po zakończeniu przetwarzania danych osobowych w danym dniu, osoba upoważniona zobowiązana jest do:
- zakończenia pracy w systemie informatycznym,
- zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.
- wylogowania się z systemu informatycznego,
- wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe,
- zamknięcia pomieszczeń.

- Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

# ROZDZIAŁ 5
## Kopie bezpieczeństwa

### § 1

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej.
Zabezpieczenie to powinno być tak skonstruowane, by umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii bezpieczeństwa.

### § 2

- Kopie zapasowe z programu CDNXL- Komarch z dysku sieciowego wykonywane są codziennie i raz w tygodniu całościowo.
- Kopie z dysków wykonywane są raz w tygodniu.
- Kopie bezpieczeństwa dokumentów ze stacji roboczych powinny być wykonywane codziennie.
- Osobą odpowiedzialną za tworzenie kopii zapasowych jest Administrator Danych Osobowych lub upoważnieni pracownicy.

Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.
Kopie bezpieczeństwa nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
Kopie bezpieczeństwa powinny być przechowywane w sejfie lub w przypadku braku takiej możliwości w zamkniętych szafach, znajdujących się w pomieszczeniach, które również są zamykane na klucz. Kopie bezpieczeństwa sa sprawdzane okresowo pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz należy je bezzwłocznie usuwać po ustaniu ich użyteczności. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.
Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

# ROZDZIAŁ 6
## Sposób i czas przechowywania oraz zasady likwidacji nośników informacji

### § 1

- Nośniki magnetyczne, optyczne i inne nośniki informatyczne, zawierające dane osobowe, przechowywane są w szafie zamykanej na klucz;
- Utworzone kopie zapasowe powinny być przechowywane w innych pomieszczeniach niż serwerownia i miejsce w którym odbywa się ;
- Do miejsca przechowywania nośników informacji i kopii zapasowych dostęp mają tylko osoby upoważnione;
- Likwidacja wydruków z systemu, zawierających dane osobowe odbywa się za pomocą

niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych;
- Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane.

# ROZDZIAŁ 7
## Ochrona antywirusowa

### § 1

- Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego wersja : Esset Etpoint Antivirus;
- Ochroną objęte są wszystkie stacje robocze;
- Aktualizacja wykonywana jest automatycznie;
- W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie osobę odpowiedzialną za nadzór nad naruszeniami;
- System informatyczny podlega regularnej, (co najmniej raz w tygodniu) kontroli pod kątem obecności wirusów komputerowych.
- Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
- Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
- Osobą odpowiedzialną za powyższe działania jest Administrator Danych Osobowych.

# ROZDZIAŁ 8
## Konserwacja i naprawa systemu przetwarzającego dane osobowe

### § 1

- Prace bieżące w dziedzinie konserwacji i naprawy systemu przetwarzającego dane na których przetwarzane są dane osobowe prowadzi ADO lub w wypadku konieczności zaangażowania do w/w czynności przedsiębiorcy zajmującego się zawodowo ich wykonywaniem, są one wykonywane pod bezpośrednim nadzorem ADO.
- Urządzenia komputerowe, dyski twarde, lub inne informatyczne nośniki danych przeznaczone do naprawy, pozbawia się przed tymi czynnościami zapisu zgromadzonych na nich danych osobowych.
- Dziennik konserwacji i napraw stanowi **załącznik nr 5** do niniejszej Instrukcji.

# ROZDZIAŁ 9
## Sposoby postępowania w zakresie komunikacji w sieci komputerowej

### § 1

- Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone hasłem.
- W miarę możliwości, dane osobowe zawarte na serwerze sieciowym nie mogą być przechowywane na stacjach roboczych. Należy dane te umieszczać na dysku sieciowym.
- Nieuzasadnione kopiowanie danych z serwera na stacje robocze, bądź na nośniki

informatyczne jest zabronione.

# ROZDZIAŁ 10

## Postępowanie w sytuacji stwierdzenia naruszenia ochrony danych osobowych

### §1

Naruszeniem zabezpieczeń systemu informatycznego są w szczególności:

- naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania danych osobowych – przez osoby nieuprawnione do dostępu do sieci lub aplikacji ze zbiorem danych osobowych;
- naruszenie lub próba naruszenia integralności danych osobowych w systemie przetwarzania (wszelkie dokonane lub usiłowane modyfikacje, zniszczenia, usunięcia danych osobowych przez nieuprawnioną do tego osobę);
- celowe lub nieświadome przekazanie zbioru danych osobowych osobie nieuprawnionej do ich otrzymania;
- nieautoryzowane logowanie do systemu;
- nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
- istnienie nieautoryzowanych kont dostępu do danych osobowych;
- włamanie lub jego usiłowanie z zewnątrz sieci;
- nieautoryzowane zmiany danych w systemie;
- nie zablokowanie dostępu do systemu przez osobę uprawnioną do przetwarzania danych osobowych w czasie jej nieobecności;
- ujawnienie indywidualnych haseł dostępu użytkowników do systemu;
- brak nadzoru nad serwisantami lub innymi pracownikami przebywającymi w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych;
- nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
- kradzież nośników, na których zapisane są dane osobowe;
- nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
- niewykonanie kopii bezpieczeństwa w odpowiednim terminie;
- niewłaściwe bądź nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe.

### § 2

W przypadkach, o których mowa w § 1, należy podjąć czynności zmierzające do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów przestępstwa i minimalizacji zaistniałych szkód.

### § 3

Osoba odpowiedzialna zobowiązana jest do niezwłocznego podjęcia działań mających na celu powstrzymanie lub ograniczenie osobom niepowołanym dostępu do danych osobowych w szczególności przez:

- zmianę hasła dla administratora i użytkowników;
- fizyczne odłączenie urządzeń i tych segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;

- wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

**§ 4**

W przypadku uszkodzenia urządzeń służących do przetwarzania danych, utraty danych, lub ich zniekształcenia, odtwarza się bazy danych osobowych z ostatniej kopii bezpieczeństwa.

# ROZDZIAŁ 11
**Postanowienia końcowe**

**§ 1**

- W sprawach nieuregulowanych niniejszą Instrukcją stosuje się przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze zm.) oraz przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
- Użytkownicy zobowiązani są do zapoznania się z niniejszą Instrukcją i do stosowania Postanowień w niej zawartych przy przetwarzaniu danych osobowych w systemach informatycznych.
- Naruszenie przez pracownika niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu Pracy odpowiedzialność pracownika.
- Instrukcja jest dokumentem wewnętrznym i nie może być udostępniona osobom postronnym.

**§ 2**

Niniejszy dokument wchodzi w życie z dniem 01.02.2018 roku.

…….....……
Administratora Danych Osobowych (ADO)

# ZAŁĄCZNIKI DO INSTRUKCJI ZARZĄDZANIA

- Wzór powołania Administratora Systemów Informatycznych
- Wykaz urządzeń
- Wniosek o nadanie/zmianę/cofnięcie uprawnień do przetwarzania danych w systemie informatycznym
- Rejestr użytkowników systemu informatycznego
- Protokół przeglądów informatycznych

załącznik nr 1

**Upoważnienie dla Administratora Systemów Informatycznych**

Administrator Danych Osobowych: WEGA-MIKOŁÓW Sp. z.o.o. Sp. K. ul. Przyjaciół 125, 43-190 Mikołów, NIP: 6351832321, REGON: 243342092
Dnia ……..2018 powołuje Pana ……. jako
Administratora Systemów Informatycznych i jednocześnie nadaje mu upoważnienie do przetwarzania danych w zbiorach danych osobowych prowadzonych przez Administratora Danych przetwarzanych za pomocą systemów informatycznych.
Upoważnienie jest ważne od chwili podpisania przez strony upoważnienia do dnia odwołania Administratora Systemów Informatycznych przez Administratora Danych Osobowych.

**ASI jest odpowiedzialny w szczególności za:**

1. wdrażanie nowych systemów informatycznych,
2. nadzorowanie poprawności przetwarzania danych w systemach informatycznych,
3. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
4. optymalizację wydajności systemu informatycznego, baz danych,
5. instalację i konfigurację sprzętu sieciowego i serwerowego,
6. instalację i konfigurację oprogramowania systemowego, sieciowego, oprogramowania bazodanowego, konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
7. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,
8. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
9. zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
10. przyznawanie za zgodą ADO ściśle określonych praw dostępu do informacji w danym systemie,
11. zarządzanie licencjami oraz procedurami ich dotyczącymi,
12. prowadzenie profilaktyki antywirusowej,
13. sprawowanie nadzoru nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
14. sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, zlecanymi firmom.

**OŚWIADCZENIE ASI**

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz że jako Administrator Systemów Informatycznych będę nadzorował przestrzeganie zasad ochrony danych zgodnie z obowiązkami wynikającymi z zapisów Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym oraz ustawy o ochronie danych osobowych.

Podpisy:

…… ……..
Administrator Danych Osobowych Administrator Systemów Informatycznych

załącznik nr 2

**Wykaz urządzeń**

| Lp. | Data wpisu | Rodzaj urządzenia, | Nr seryjny | Dział użytkujący |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| 6. | | | | |
| 7. | | | | |
| 8. | | | | |
| 9. | | | | |
| 10. | | | | |
| 11. | | | | |
| | | | | |

załącznik nr 3

**Wniosek o nadanie/zmianę/cofnięcie uprawnień**
**do przetwarzania danych w systemie informatycznym**

……..……
wnioskujący

**Wniosek**

Niniejszym wnoszę o nadanie/zmianę/cofnięcie* uprawnień dla pracownika

……..
(*podać imię i nazwisko, stanowisko służbowe*)

do dostępu do danych osobowych w zakresie systemu informatycznego w aplikacji

……..……

w zakresie uprawnień……
(*wprowadzanie danych, wgląd, edycja, kopiowanie, usuwanie*)

..... .....
czytelny podpis wnioskującego (data i podpis użytkownika)

| | |
|---|---|
| ……..<br>Podpis nadającego uprawnienia | |