INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

w

. . . . . .

[nazwa firmy]

……..

[Data sporządzenia i wdrożenia]

§1
POSTANOWIENIA OGÓLNE I DEKLARACJE ADMINISTRATORA

1. Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych ..... [nazwa firmy] przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej jako RODO).
2. Niniejsza Instrukcja stanowi załącznik do obowiązującej Polityki bezpieczeństwa przetwarzania danych osobowych u Administratora danych osobowych (Polityki ochrony danych osobowych), dalej jako Polityka.
3. Administrator zapewnia, że stosuje adekwatne środki bezpieczeństwa, które zapewniają ochronę danych osobowych przez ujawnieniem, zabraniem, zniszczeniem lub ich utratą, w szczególności mając na uwadze odpowiednią ochronę tzw. danych wrażliwych, jeśli je przetwarza lub zacznie przetwarzać w swojej działalności.
4. Wszystkie osoby przetwarzające dane osobowe w systemie informatycznym bez względu na zajmowane stanowisko i miejsce pracy zobowiązane są do postępowania zgodnie z zasadami określonymi w niniejszej Instrukcji oraz wykonywania poleceń Administratora Danych Osobowych w zakresie bezpieczeństwa systemu informatycznego.
5. Instrukcja określa w szczególności:
   a) nadawanie, zmianę i odebranie uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym, w szczególności mając na uwadze tzw. dane wrażliwe, jeśli występują;
   b) stosowane metody autoryzacji użytkownika w systemach informatycznych;
   c) ochrona przed zagrożeniami pochodzącymi z sieci publicznej;
   d) zabezpieczenie systemu informatycznego przed działalnością złośliwego oprogramowania;
   e) procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym;
   f) urządzenia drukujące stosowane w przetwarzaniu danych osobowych;
   g) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe;
   h) procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych;

   i) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   j) ochrona pomieszczeń, w których przechowywane są istotne elementy systemu informatycznego;
   k) monitorowanie systemu informatycznego.
6. Dane osobowe przetwarzane są w systemach własnych Administratora danych oraz w zasobach platformy hostingowej zarządzanej przez …………………………… (podmiot któremu powierzono przetwarzanie danych osobowych, tzw. „Procesor Danych", czy „Procesor") w:
   a) dyskach twardych serwerów bazodanowych,
   b) macierzach dyskowych,
   c) pamięci operacyjnej (RAM) serwerów,
   d) dyskach sieciowych serwerów plikowych,
   e) repozytoriach serwerów pocztowych,
   f) repozytoriach serwerów wewnętrznych systemów pomocniczych, np. Intranet,
   g) kopiach zapasowych wykonywanych na dyskach lokalnych serwerów, macierzach dyskowych i „chmurze obliczeniowej", wykorzystywanych przy wykonywaniu i składowaniu kopii,
   h) w archiwum, w którym znajduje się źródłowa dokumentacja papierowa oraz elektroniczna dotycząca przetwarzanych danych osobowych, oraz na przeznaczonych do tego celu komputerach Administratora Danych.
7. Administrator Danych Osobowych prowadzi **rejestr kont osób i systemów przetwarzających dane osobowe oraz urządzeń mobilnych** (laptopy, dyski przenośne, pendrive), służących do przetwarzania danych osobowych.

ZAŁĄCZNIK: Rejestr kont osób i systemów przetwarzających dane osobowe oraz urządzeń mobilnych

§2
DEFINICJE

1. **Administrator Danych Osobowych lub Administrator Danych lub Administrator -** . . . . [nazwa działalności gospodarczej – imię, nazwisko, firma]
2. **Dane osobowe zwykłe lub Dane osobowe –** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio,

w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników, określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne, np.: imię, nazwisko, numer PESEL, adres e-mail, data urodzenia, adres zamieszkania.

3. **Dane osobowe wrażliwe** – dane osobowe, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, stan zdrowia i wszelkie informacje dotyczące zdrowia psychicznego lub fizycznego, kod genetyczny, dane genetyczne i biometryczne, nałogi lub życie seksualne, dotyczące skazań, orzeczeń o ukaraniu, mandatów karnych.
4. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych
5. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych. Użytkownikiem może być pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej.
6. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
7. **Odbiorca danych –** każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a) Osoby, której dane dotyczą,
   b) Osoby upoważnionej do przetwarzania danych,
   c) Podmiotu, któremu powierzono przetwarzanie danych,
   d) Organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
8. **Osoba upoważniona –** osoba, która została upoważniona przez Administratora danych osobowych do przetwarzania danych w celu i w zakresie wskazanym w upoważnieniu. Może nią być osoba zatrudniona na podstawie umowy o pracę, umowy cywilnoprawnej, wolontariusz, stażysta.
9. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy jest rozproszony, czy podzielony funkcjonalnie.
10. **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. Zasady zawarte w niniejszej Polityce należy stosować przy każdej operacji na danych.

11. **Udostępnienie danych** – przekazanie danych osobowych innemu administratorowi danych na podstawie właściwych przepisów prawa, np. sądowi, policji, prokuraturze.
12. **Powierzenie danych –** przekazanie danych osobowych innemu podmiotowi w określonym celu i zakresie, na podstawie zawartej umowy i w ramach jej realizacji, np. umowy z biurem rachunkowym.
13. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie.
14. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika) w systemach informatycznych, najczęściej polegające na wpisaniu loginu i hasła użytkownika.
15. **RODO** – oznacza Rozporządzenie Parlamentu Europejskiego i Rady EU 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).

§3
PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

1. Za bezpieczeństwo Danych osobowych w Systemie informatycznym

   . . . . . [nazwa systemu] i za właściwy nadzór odpowiedzialny jest Administrator Danych Osobowych.
2. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych, na zasadach określonych w niniejszej Instrukcji i Polityce bezpieczeństwa.
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany **Identyfikator użytkownika**. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i Hasło.
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.

6. Identyfikator osoby, która utraciła uprawnienia do dostępu do Danych osobowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
7. Każda upoważniona osoba przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zobowiązana jest zapoznać się z:
   a) postanowieniami ustawy o ochronie danych osobowych,
   b) polityką bezpieczeństwa przetwarzania danych osobowych u Administratora danych,
   c) obowiązującą u Administratora danych **Instrukcją postępowania w przypadku wystąpienia incydentu związanego z naruszeniem zasad ochrony danych osobowych,**
   d) niniejszą Instrukcją.
8. Fakt zapoznania się z przepisami, o których mowa w ust. 7, operator danych zobowiązany jest potwierdzić własnoręcznym podpisem we właściwym dokumencie, przedstawionym mu do podpisania przez Administratora Danych.

9. Teksty wszystkich wymienionych dokumentów i aktów prawnych znajdują się do wglądu w siedzibie firmy.

§4
METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Instrukcję stosuje się do stacji roboczych, komputerów przenośnych, pozostałych urządzeń mobilnych (telefony, tablety), serwerów, sieci informatycznej oraz pozostałych elementów Systemu informatycznego.
2. Dane osobowe w komputerach przenośnych i urządzeniach mobilnych mogą być przetwarzane wyłącznie za zgodą Administratora Danych Osobowych i dopuszczalne jest to wyłącznie, gdy dostęp do systemu operacyjnego urządzenia jest zabezpieczony hasłem i pozostałymi środkami ochrony wobec przetwarzanych danych osobowych.
3. W Systemie informatycznym stosuje się Uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do Uwierzytelnienia Użytkownika na poziomie dostępu do systemu operacyjnego stosuje się Hasło oraz Identyfikator użytkownika.
4. Hasła użytkowników umożliwiające dostęp do Systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.

5. Użytkownik jest zobowiązany do niekorzystania z opcji przechowywania hasła w pamięci przeglądarki internetowej, a także niezapisywania hasła w miejscach dostępnych dla osób trzecich.
6. Minimalna długość Hasła przydzielonego Użytkownikowi wynosi ……. znaków alfanumerycznych i znaków specjalnych.
7. Zabrania się używania Identyfikatora lub Hasła innej osoby.
8. Dla każdej osoby, której Dane osobowe są przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:
   a)daty pierwszego wprowadzenia danych do systemu,
   b)identyfikatora Użytkownika wprowadzającego Dane osobowe do systemu,
   c)informacji o odbiorcach, którym Dane osobowe zostały udostępnione.
9. Podczas transportu, przechowywania i użytkowania urządzenia przenośnego poza obszarem przetwarzania, zawierającego dane osobowe, Użytkownik komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności.
10. Administrator Danych Osobowych odpowiada za aktualizację systemów operacyjnych i aplikacji. Wszelkie zmiany w Systemie informatycznym mogą być dokonywane wyłącznie za jego zgodą lub przez upoważnioną przez niego osobę.
11. Administrator Danych Osobowych lub upoważniona przez niego osoba blokuje dostęp do systemu użytkownikom, którzy kończą współpracę lub których obowiązki nie wymagają już korzystania z danego Systemu informatycznego.

§5
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU

1. Po przyjściu do pracy Użytkownik uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu Użytkownik loguje się przy pomocy Identyfikatora Użytkownika oraz Hasła do Systemu informatycznego.
4. Rozpoczynając pracę Użytkownik zobowiązany jest dopilnować, czy załadowało się oprogramowanie antywirusowe monitorujące komputer, jeśli takie jest dostępne.
5. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.
6. Użytkownik jest zobowiązany do stosowania tzw. **polityki czystego ekranu**, polegającej na uniemożliwieniu dostępu osobom nieupoważnionym do informacji wyświetlanych na

ekranie komputera poprzez właściwe ustawienie monitora oraz blokowanie dostępu do urządzenia, kiedy Użytkownik opuszcza stanowisko pracy.

7. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 minutach braku aktywności).
8. Użytkownik zobowiązany jest wylogować się ze wszystkich aplikacji, z których korzystał, wyłączyć stację roboczą i monitor oraz zabezpieczyć wszelkie wykorzystywane nośniki danych, jeśli kończy pracę w systemie informatycznym.
9. Wszelkie zauważone okoliczności wskazujące na możliwość naruszenia bezpieczeństwa danych osobowych muszą zostać bezzwłocznie zgłoszone do Administratora Danych.
10. W uzasadnionych przypadkach Użytkownicy mogą uzyskać od Administratora Danych lub Procesora zgodę na odstępstwa od zasad opisanych w niniejszym paragrafie, w zakresie konieczności wylogowywania się z aplikacji lub systemów.

§6

TWORZENIE KOPII ZAPASOWYCH ZBIORÓW DANYCH

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Administratora.
2. Do archiwizacji służą …….. [dyski DVD/ dyski zewnętrzne/ chmura obliczeniowa/itp.]
3. Wszystkie dane archiwizowane powinny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisane w kopii danych.
4. Kopie zapasowe przechowuje się w sposób zabezpieczający je przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem, zabraniem lub zniszczeniem.
5. W szczególności należy wykonywać następujące kopie bezpieczeństwa:

   1) przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,

   2) przed dokonaniem zmian w programach (np. zmiana wersji),

   3) po każdej istotnej zmianie danych w bazie danych.

6. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz na kwartał poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

§7

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są przeznaczone. Po upływie tego okresu dane podlegają usunięciu lub anonimizacji, o ile w odniesieniu do nich nie obowiązują przepisy prawa uprawniające do ich przetwarzania w celu archiwizacji lub sprawozdawczości finansowej.
5. Dane osobowe przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, jedynie przez okres niezbędny do spełnienia celu, w jakim zostały na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika podlega usunięciu przy użyciu narzędzi zaakceptowanych do użycia przez Administratora Danych Osobowych.
6. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
7. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

§8

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁANIEM WIRUSÓW KOMPUTEROWYCH, NIEUPRAWNIONYM DOSTĘPEM ORAZ AWARIAMI ZASILANIA

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:

	Obszar chroniony	Rodzaj ochrony	Typ

1.	*Stacje robocze*	*System antywirusowy*	…
2		*Firewall*	…
3		*Szyfrowanie nośników danych*	…
4.	*Sieć we-wnętrzna*	*System antywirusowy*	…
5		*Firewall*	…
6.	*Poczta e-mail*	*Szyfrowanie danych*	…
7		*System antiwirusowy i antyspamowy*	…

2. Użytkowany system jest automatycznie skanowany z częstotliwością ……..
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy:
   a) uruchomić program antywirusowy i skontrolować użytkowany system,
   b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.

   Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
   a) zakończyć pracę w systemie komputerowym,
   b) odłączyć zainfekowany komputer od sieci,
   c) powiadomić o zaistniałej sytuacji Administratora Danych lub Inspektora Ochrony Danych Osobowych (jeśli został wyznaczony).
5. Użytkownikom nie wolno korzystać z nośników przenośnych, podłączania nieautoryzowanych dysków zewnętrznych, pendrive lub podłączać komputerów do nieautoryzowanych sieci zewnętrznych bez zgody Administratora Danych Osobowych.
6. Użytkownikom zabrania się uruchamiania lub pobierania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku przez Administratora Danych Osobowych lub osobę przez niego do tego upoważnioną.
7. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

8. W celu ochrony przed działaniem złośliwego oprogramowania Administrator Danych Osobowych dodatkowo stosuje filtry antyspamowe, monitorowanie działań użytkowników, blokowanie stron potencjalnie niebezpiecznych lub zablokowanie możliwości podłączenia nieautoryzowanych urządzeń zewnętrznych.

§9
POCZTA ELEKTRONICZNA I OCHRONA PRZED ZAGROŻENIAMI POCHODZĄCYMI Z SIECI PUBLICZNEJ

1. Pracownicy/współpracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. *phishing e-mail*). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.
4. Administrator Danych Osobowych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej, np. certyfikaty SSL.
5. Administrator Danych Osobowych zabezpiecza systemy informatyczne, służące do przetwarzania danych osobowych, przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie zabezpieczeń chroniących przed nieuprawnionym dostępem, co obejmuje kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną.

§10
SPOSOBY REALIZACJI W SYSTEMIE WYMOGÓW DOTYCZĄCYCH PRZETWARZANIA DANYCH (ZAPISANIE W SYSTEMIE INFORMATYCZNYM INFORMACJI O ODBIORCACH DANYCH)

1. Informacje o odbiorcach danych zapisywane są w Systemie informatycznym, z którego nastąpiło udostępnienie przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.

2. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

§11

OCHRONA OBSZARU PRZETWARZANIA DANYCH

1. Administrator Danych Osobowych zabezpiecza w sposób adekwatny pomieszczenia, w których znajdują się elementy sieci komputerowych, takie jak serwery, urządzenia sieciowe, modemy, w sposób uniemożliwiający dostęp osobom trzecim.
2. Przebywanie w obszarze przetwarzania osób nieupoważnionych do danego systemu informatycznego jest możliwe tylko w obecności użytkownika upoważnionego, znajdującego się w danym pomieszczeniu, przedstawiciela Administratora lub Procesora, albo Administratora.
3. Drzwi wejściowe do pomieszczeń obszaru przetwarzania danych muszą pozostawać zamknięte zarówno po zakończeniu pracy przez osoby upoważnione, jak i w wypadku każdego, opuszczenia przez nie pomieszczenia w ciągu czasu pracy.
4. W przypadku opuszczenia pomieszczenia osoba upoważniona zobowiązana jest do zabrania ze sobą klucza do drzwi lub karty dostępu którą dysponuje i zabezpieczenia pomieszczenia przed dostępem osób nieupoważnionych.
5. W przypadku utraty klucza lub karty dostępu osoba upoważniona zobowiązana jest do natychmiastowego poinformowania o tym fakcie Administratora Danych.
6. Do przesłanek wskazujących na naruszenie bezpieczeństwa ochrony danych należą m. in.:
   a) próby błędnych logowań do systemów przetwarzających dane osobowe,
   b) próby nieautoryzowanego dostępu do baz danych,
   c) próby wynoszenia danych na nośnikach pamięci masowych,
   d) pozostawienie wydruków danych osobowych na drukarkach, kserokopiarkach lub innych urządzeniach poligraficznych lub w miejscach niechronionych,
   e) wysyłanie, przez osoby nieupoważnione, dokumentów lub informacji zawierających dane osobowe za pośrednictwem poczty elektronicznej lub konwencjonalnej oraz urządzeń teletransmisyjnych.
7. W przypadku drukowania dokumentów zawierających dane osobowe z systemu informatycznego, Użytkownik jest zobowiązany zwrócić uwagę na niepozostawianie jakichkolwiek wydruków i dokumentów na ogólnodostępnych urządzeniach drukujących,
   w szczególności po wydrukowaniu, kopiowaniu lub skanowaniu.
8. Użytkownik, który generuje wydruk odpowiada za jego dalsze przetwarzanie poza systemem informatycznym.

9. Gdy dalsze przetwarzanie wydruku zawierającego dane osobowe nie jest już konieczne podlega on niezwłocznemu i trwałemu niszczeniu w sposób uniemożliwiający odtworzenie jego treści.

§12
PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez Administratora Danych lub firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań (umowy powierzenia danych).
2. Jeśli systemy informatyczne zawierają dane osobowe i wykonanie przeglądu lub konserwacji odbywa się z udziałem podmiotu zewnętrznego to Administrator Danych Osobowych dopilnowuje zawarcia umowy powierzenia danych.
3. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
   a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych,
   a) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
   b) przegląd lub konserwacja są poprzedzone wykonaniem kopii bezpieczeństwa danych,
   c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,
   d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.
5. Przekazanie sprzętu informatycznego do serwisu lub naprawy poza teren przetwarzania Administratora Danych Osobowych jest dopuszczalne wyłącznie pod warunkiem, że sprzęt przekazywany pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie lub podpisania umowy powierzenia przetwarzania danych, jeśli usunięcie danych nie jest możliwe.

6. Jeśli niszczenia nośników danych dokonują wyspecjalizowane podmioty zewnętrzne to Administrator Danych Osobowych jest zobowiązany do udokumentowania zdarzenia zniszczenia nośników odpowiednim protokołem, uzyskanym od tego podmiotu.
7. Jeśli urządzenia informatyczne nie mogą zostać pozbawione zapisu danych osobowych to Administratorowi Danych Osobowych zawiera umowę powierzenia danych w celu przeprowadzenia ich niszczenia.

§13
REJESTRACJA I MONITORING DOSTĘPU DO SYSTEMÓW PRZETWARZANIA DANYCH OSOBOWYCH

1. Każdorazowy dostęp do baz danych osobowych oraz serwerów, na których przetwarzane są dane osobowe jest odnotowywany w logach/rejestrach. System rejestracji w pełni pozwala na identyfikację tożsamości operatora danych, aplikacji lub administratora, który w danym czasie uzyskał dostęp do systemów przetwarzających dane osobowe i/lub dokonał operacji na danych.
2. Administrator Danych, a na jego zlecenie Procesor, lub osoba przez nich wyznaczona, zobowiązani są do bieżącego monitorowania logów. Wszelkie próby nieuprawnionego dostępu muszą być zgłaszane Administratorowi Danych zgodnie z **Instrukcją postępowania w przypadku wystąpienia incydentu związanego z naruszeniem zasad ochrony danych osobowych,** zawartą w Polityce bezpieczeństwa**.**
3. Kopie zapasowe logów/rejestrów są tworzone automatycznie i powinny być przechowywane.

§14
PROCEDURA USUWANIA AWARII SPRZĘTU LUB OPROGRAMOWANIA

1. W przypadku wystąpienia awarii Systemu Informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii Administratorowi Danych lub osobie odpowiedzialnej za obsługę informatyczną.
2. Administrator danych lub osoba odpowiedzialna za obsługę informatyczną zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.
3. Po usunięciu awarii Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
   a) uruchomienia Systemu Informatycznego;
   b) kontroli poprawności jego funkcjonowania;
   c) kontroli integralności danych.

4. W przypadku stwierdzenia uszkodzenia danych zgromadzonych w Systemie, administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).
5. W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu Administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, osoba przekazująca sprzęt ze strony salonu zobowiązana jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności.

§15
POSTANOWIENIA KOŃCOWE

1. Wszystkie czynności związane z przetwarzaniem danych u Administratora danych osobowych, które nie zostały opisane w niniejszej Instrukcji, są nadzorowane przez Administratora Danych.
2. Administrator Danych posiada uprawnienia do zmian regulacji wynikających z niniejszego dokumentu.
3. Administrator Danych może powierzyć (osobie trzeciej, w tym Procesorowi lub innej osobie lub podmiotowi) całość lub część czynności związanych z nadzorem nad funkcjonowaniem części lub całości systemów i procesów związanych z przetwarzaniem danych osobowych w ramach prowadzonej działalności. W każdym przypadku na Administratorze Danych lub osobie przez niego upoważnionej ciąży obowiązek kontrolowania właściwego wykonywania czynności związanych z przetwarzaniem danych osobowych.
4. Treść niniejszej Instrukcji ma charakter informacji stanowiącej tajemnicę przedsiębiorstwa, zgodnie z art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) oraz chronionej tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt 4 Kodeksu pracy (t.j. Dz. U. z 2016 r., poz.1666 ze zm.). Wybrane elementy Instrukcji mogą zostać udostępnione partnerom po zawarciu stosownej umowy o zachowaniu poufności.
5. Z treścią niniejszego dokumentu powinni być zapoznani wszystkie osoby upoważnione do przetwarzania danych osobowych.

……..……..

[data i podpis Administratora Danych Osobowych]