POLITYKA BEZPIECZEŃSTWA INFORMACJI

MIETEX Sp. z o.o.
ul. Fabryczna 1, 47-208 Reńska Wieś
NIP 7492114930, REGON 523259581

Reńska Wieś, dnia 02 kwietnia 2024 r.

ROZDZIAŁ I
POSTANOWIENIA OGÓLNE

§ 1

1. Niniejsza *Polityka Bezpieczeństwa Informacji*, zwana dalej *Polityką Bezpieczeństwa*, została sporządzona w celu zapewnienia przetwarzania i zabezpieczenia danych osobowych w ramach działalności gospodarczej MIETEX Sp. z o.o., zgodnie z przepisami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym w szczególności zgodnie z:
   1) ustawą z 29 sierpnia 1997 r. *o ochronie danych osobowych* (tekst jedn. Dz.U z 2016 r. poz. 922 z późn. zm.),
   2) ustawa z 10 maja 2018 r. *o ochronie danych osobowych* (tekst jedn. Dz.U. z 2018 r. poz. 1000 z późn. zm.),
   3) rozporządzeniem 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* (Dz.U. L. 119/1 z 4.5.2016, s. 1-88) – dalej jako: *Rozporządzenie RODO*,
   4) przepisami wykonawczymi do ustawy, o której mowa w pkt 1 i 2.
2. *Polityka Bezpieczeństwa* dotyczy wszystkich danych osobowych przetwarzanych w ramach działalności gospodarczej MIETEX Sp. z o.o., niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
3. *Polityka Bezpieczeństwa* określa w szczególności:
   1) prawa, obowiązki oraz granice dopuszczalnego zachowania osób przetwarzających dane osobowe w związku z działalnością gospodarczej MIETEX Sp. z o.o., użytkowników systemów informatycznych, w których przetwarzane są dane osobowe oraz konsekwencje naruszenia przepisów o ochronie danych osobowych,
   2) sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych, w tym podstawowe warunku jakim powinny odpowiadać urządzenia z wykorzystaniem których dane są przetwarzane,
   3) zasady prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych,
   4) zasady prowadzenia wykazu zbiorów danych osobowych,
   5) wymagania w zakresie odnotowywania udostępniania danych osobowych,
   6) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych.
4. Postanowienia *Polityki Bezpieczeństwa* zmierzają do zapewniania w ramach działalności gospodarczej MIETEX Sp. z o.o.:
   1) poufności danych – rozumianej jako właściwość zapewniającą, że dane osobowe są udostępniane wyłącznie upoważnionym podmiotom,
   2) integralności danych – rozumianej jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) rozliczalności danych – rozumianej jako właściwość zapewniająca, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   4) integralności systemu – rozumianej jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej,
   5) dostępności informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to niezbędne,
   6) zarządzania ryzykiem – rozumianego jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.

§ 2

Zasady i sposób postępowania pracowników i pozostałych członków personelu działalności gospodarczej MIETEX Sp. z o.o. w związku z przetwarzaniem danych osobowych w systemach informatycznych uregulowany został w *Instrukcji zarządzania systemem informatycznym*, która stanowi *Załącznik nr 1* do *Polityki Bezpieczeństwa*.

§ 3

Użyte w ramach *Polityki Bezpieczeństwa* wyrażenia oznaczają:

1) Administrator Danych – MIECZYSŁAW MATYJEWICZ, prowadzący działalność gospodarczą pod nazwą MIETEX Sp. z o.o., ul. Fabryczna 1, 47-208 Reńska Wieś, NIP 7492114930, REGON 523259581,
2) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, 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,
3) działania korygujące – działania przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności (incydentu) lub innej niepożądanej sytuacji,
4) działania zapobiegawcze – działanie, które należy przedsięwzięć, aby wyeliminować przyczyny potencjalnej niezgodności (incydentu) lub innej niepożądanej sytuacji,
5) incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócania działania systemu informatycznego i zagrażają bezpieczeństwu informacji; naruszenia bezpieczeństwa informacji ze względu na poufność, dostępność i integralność,
6) niezgodność – niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe,
7) nośniki danych – przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji,
8) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych,
9) użytkownik – osoba upoważniona przez Administratora Danych do przetwarzania danych osobowych w ramach systemu informatycznego,
10) zbiór danych – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów,
11) 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,
12) uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (użytkownika),
13) profilowanie – automatyczny proces przetwarzania danych osobowych,
14) teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
15) zagrożenie – potencjalna możliwość wystąpienia incydentu,
16) zdarzenie – błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z zagrożeniem bezpieczeństwa danych osobowych,
17) procesor – podmiot, któremu powierza się dalsze przetwarzanie danych osobowych na podstawie stosownego postanowienia w umowie, zapewniającego warunki bezpieczeństwa danych

osobowych zgodnie z przepisami lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych,

18) personel – podmioty zaangażowane w ramach działalności gospodarczej MIETEX Sp. z o.o., w tym osoby zatrudnione na podstawie stosunku pracy (pracownicy), umów cywilnoprawnych, przedsiębiorców wykonujących działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażystów, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej,
19) osobie upoważnionej do przetwarzania danych osobowych – pracownik lub inny członek personelu upoważnionego na piśmie do przetwarzania danych osobowych,
20) anonimizacja – przekształcenie danych osobowych, po którym niemożliwe jest przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej.

ROZDZIAŁ II
ZASADY POZYSKIWANIA ORAZ PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ ADMINISTRATORA DANYCH OSOBOWYCH

§ 4

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator Danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator Danych wykona czynności określone w art. 35 i nast. *Rozporządzenia RODO*, w tym w szczególności wykona analizy ryzyka oraz celowości zastosowania określonych środków ochrony.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi *Załącznik nr 2* do *Polityki Bezpieczeństwa*.

§ 5

1. Wszystkie dane osobowe w ramach działalności Administratora Danych są zbierane i przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa.
2. Dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Administrator Danych może żądać podania jedynie tych danych, które są niezbędne do realizacji jego celów i zadań, w jakich spełniony jest co najmniej jeden z poniższych warunków:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub w większej liczbie określonych celów,
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą,
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze Danych,
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub innej osoby,
   5) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

3. Administrator Danych nie zbiera i nie przetwarza danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, za wyjątkiem sytuacji, o których mowa w art. 6 ust. 2 *Rozporządzenia RODO*, w tym w szczególności wyraźnej zgody osoby, której dane dotyczą bądź wymagają tego obowiązujące przepisy prawa.
4. Administrator Danych zbiera i przetwarza dane o niekaralności wyłącznie w zakresie niezbędnym do zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej.
5. Dane są przetwarzane w sposób rzetelny i przejrzysty, wyłącznie dla celów, dla jakich były, są lub będą zbierane i przetwarzane.
6. Dane są prawidłowe i w razie potrzeby uaktualniane.
7. Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane oraz przez czas przedawnienia ewentualnych roszczeń. Po tym okresie dane są trwale usuwane lub animizowane, co zostanie potwierdzone protokołem, którego wzór stanowi *Załącznik nr 4b.*
8. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikacje osób, których dotyczą, zniszczone lub w przypadku powierzenia, zwrócone podmiotowi, który dane powierzył.

§ 6

1. Do profilowania zabrania się używania danych wrażliwych, o których mowa w § 5 ust. 3 i 4 *Polityki Bezpieczeństwa,* chyba że wymagają tego obowiązujące przepisy prawa, osoba, której dane dotyczą wyraziła na to zgodę, lub jest to podyktowane ważnym interesem publicznym.
2. Przy profilowaniu Administrator Danych obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osób, których dane dotyczą.
3. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą.
4. Każda osoba, której dane dotyczą ma prawo wyrażenia sprzeciwu na profilowanie jej danych osobowych jeżeli uzna, że to jej prawa i wolności.

§ 7

1. Wymaga się, aby zgoda na przetwarzanie danych osobowych, o której mowa w § 5 ust. 2 pkt 1 oraz § 5 ust. 4 *Polityki Bezpieczeństwa* stanowiła dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
2. Zgoda na przetwarzanie danych powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach, jeżeli przetwarzanie służy różnym celom, należy pozyskać odrębną zgodę na każdy cel.
3. Zgoda na przetwarzanie danych osobowych, może być odwołana w każdym czasie w sposób tak samo prosty i przystępny, w jaki została pozyskana.

§ 8

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu i zakresie zbierania danych, a w szczególności i znanych mu w czasie udzielenia informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej i konsekwencjach niepodania danych,
4) prawnie uzasadnionym interesie Administratora Danych, jeżeli na tej podstawie odbywać się będzie przetwarzanie danych,
5) okresie, przez które dane osobowe będą przechowywane lub o kryterium tego okresu,
6) profilowaniu danych,
7) prawach osoby, której dane dotyczą, tj. prawie do usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych), wniesienia skargi do organu nadzoru.

2. W przypadku pozyskiwania danych osobowych z innego źródła niż osoba, której dane dotyczą, Administrator Danych jest zobowiązany poinformować tę osobę, oprócz informacji wskazanych w ust. 1, o źródle pozyskania danych oraz przysługujących tej osobie uprawnieniach.
3. Obowiązek, o którym mowa w ust. 1 powinien być wykonany w momencie zbierania danych, z wyjątkiem sytuacji, w której przepis innej ustawy zezwala na przetwarzanie danych osobowych lub osoba, której dane dotyczą posiada już informacje.
4. Obowiązek, o którym mowa w ust. 2 powinien być wykonany bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie.

§ 9

1. Wzory zgód wraz z obowiązkowymi formularzami informacyjnymi stanowią *Załączniki nr 3a, 3b i 3c* do *Polityki Bezpieczeństwa:*
   1) *Załącznik nr 3a* – wzór zgody na przetwarzanie danych osobowych,
   2) *Załącznik nr 3b* – wzór zgody na przetwarzanie danych osobowych pracownika lub innego członka personelu w celach kadrowych,
   3) *Załącznik nr 3c* – wzór zgody na przetwarzanie danych osobowych w celu wykonywania umowy.
2. W celu wypełnienia obowiązków, o których mowa w § 8 ust. 1 w zw. z § 5 ust. 2 pkt 2 Administrator Danych może przekazać osobie, której dane są przetwarzane, w formie papierowej, elektronicznej lub poprzez umieszczenie na innym dokumencie oświadczenia, którego wzór stanowi *Załącznik nr 3d* do *Polityki Bezpieczeństwa*.

§ 10

Przetwarzanie danych osobowych odbywa się w szczególności z wykorzystaniem dokumentów, materiałów, przesyłek analogowych (nieelektronicznych), pism, akt osobowych pracowników, dokumentów finansowo-księgowych, dokumentów prawnych oraz danych zawartych na nośnikach elektronicznych, magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych, a także danych przetwarzanych w systemie kadrowo-płacowym, systemie do obsługi dokumentów księgowych, wymianie informacji z organami administracji publicznej i samorządowej oraz obsługą prawną i księgową Administratora Danych.

§ 11

1. Wszystkie osoby, które posiadają dostęp do danych osobowych zebranych oraz przetwarzanych w ramach działalności Administratora Danych muszą posiadać upoważnienie do przetwarzania danych osobowych oraz podpisać oświadczenie o zachowaniu poufności.
2. Administrator Danych prowadzi wykaz udostępnień danych osób upoważnionych do przetwarzania danych osobowych.

3. Wzór upoważnienia wraz oświadczenia, o którym mowa w ust. 1, określony został w *Załączniku nr 4* do *Polityki Bezpieczeństwa.*
4. Wzór wykazu, o którym mowa w ust. 2 określony został *w Załączniku nr 5* do *Polityki Bezpieczeństwa.*

ROZDZIAŁ III
PRAWA I OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

§ 12

1. Funkcję Administratora Danych sprawują Mieczysław Matyjewicz lub osoba przez niego upoważniona.
2. Administrator Danych podejmuje decyzje w zakresie realizacji celów i zapewnienia środków zapewniających bezpieczeństwo przy przetwarzaniu danych osobowych, zgodnie z wymogami i zaleceniami wynikającymi z przepisów prawa, w celu ochrony interesów osób, których dane dotyczą.

§ 13

1. Administrator Danych realizuje zadania z zakresu ochrony danych osobowych, nadzorując przestrzeganie zasad ochrony danych osobowych w ramach jego działalności, w tym zwłaszcza zadania polegające na:
   1) sprawowaniu stałego nadzoru nad bezpieczeństwem i ochroną danych osobowych zgodnie z wymogami przepisów prawa,
   2) zapewnieniu przetwarzania danych osobowych zgodnie z postanowieniami *Polityki Bezpieczeństwa* i *Instrukcji zarządzania systemem informatycznym*,
   3) sprawowaniu stałego nadzoru nad przestrzeganiem przez pracowników zasad ochrony danych osobowych określonych w *Polityce Bezpieczeństwa* oraz *Instrukcji zarządzania systemem informatycznym*,
   4) sprawowaniu stałego nadzoru nad wdrożeniem i stosowaniem odpowiednich środków fizycznych, technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych zgodnie z wymogami prawa,
   5) nadawaniu, modyfikowaniu oraz odwoływaniu, upoważnień do przetwarzania danych osobowych oraz zasad i przetwarzania danych osobowych oraz prowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych,
   6) udzielaniu pracownikom informacji i wyjaśnień dotyczących przepisów o ochronie danych osobowych i zasad ich ochrony obowiązujących w ramach jego działalności,
   7) przeprowadzeniu sprawdzeń i wewnętrznych kontroli przestrzegania przepisów o ochronie danych osobowych,
   8) prowadzaniu i aktualizacji dokumentacji opisującej sposób przetwarzania danych osobowych oraz stosowane środki techniczne i organizacyjne zapewniające ochronę danych osobowych, w tym *Polityki Bezpieczeństwa* i *Instrukcji zarządzania systemem informatycznym*,
   9) nadzorowaniu powierzania przetwarzania danych osobowych innym podmiotom, w szczególności nadzorowaniu spełniania wymagań zasad ochrony danych osobowych,
   10) nadzorowaniu udostępnień danych osobowych,
   11) prowadzeniu wszelkich ustaleń z Prezesem Urzędu Ochrony Danych Osobowych oraz Urzędem Ochrony Danych Osobowych,
   12) przygotowaniu wszelkich dokumentów dotyczących ochrony danych osobowych,
   13) inicjowaniu i wspieraniu przedsięwzięć w zakresie doskonalenia ochrony danych osobowych, w tym zwłaszcza przeprowadzaniu szkoleń z zakresu ochrony danych osobowych,

14) zapewnieniu środków niezbędnych wykonywania obowiązków wynikających z zasad ochrony danych osobowych,
15) podejmowaniu odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych.

2. W celu prawidłowego wykonywania zadań, o których mowa w ust. 1, Administrator Danych jest uprawniony do:
   1) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych osobowych i przeprowadzenia wszelkich niezbędnych czynności kontrolnych w celu oceny zgodności przetwarzania danych,
   2) żądania od pracowników, w tym osób upoważnionych, złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego dotyczącego przetwarzania danych i ich zabezpieczenia,
   3) żądania udostępnienia do kontroli zgodności przetwarzania danych z przepisami o ochronie danych dokumentacji, urządzeń i nośników oraz systemów informatycznych służących przetwarzaniu danych osobowych,
   4) prowadzenie działań kontrolnych u procesora w zakresie zgodności przetwarzania powierzonych danych z przepisami o ochronie danych i umowie o powierzeniu danych, w tym także żądania okazania dokumentów,
   5) występowanie do procesora o wyjaśnienia i informacje dotyczące przetwarzania danych osobowych,
   6) wyznaczenia, rekomendowania i egzekwowania od pracowników wykonania zadań związanych z ochroną danych osobowych,
   7) wydawania pracownikom wiążących zadań związanych z ochroną danych osobowych.

§ 14

1. Administrator danych realizuje zadania w zakresie ochrony danych osobowych również poprzez nadzorowanie funkcjonowania i eksploatacji systemu informatycznego służącego do przetwarzania danych osobowych w ramach jego działalności, w tym zwłaszcza:
   1) zapewnia prawidłowe funkcjonowanie i eksploatację systemu informatycznego, zgodnie z celami przetwarzania danych osobowych,
   2) przyznaje uprawnionym użytkownikom systemu identyfikator oraz hasło do systemu, a także w razie konieczności lub potrzeby dokonuje ewentualnych modyfikacji uprawnień bądź usuwa konta użytkowników,
   3) przeciwdziała dostępowi osób nieuprawnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,
   4) nadzoruje prawidłowe działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
   5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
   6) wykonuje oraz sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją sprzętu i urządzeń wchodzących w skład systemu informatycznego, na których przetwarzane są dane osobowe,
   7) wykonuje oraz sprawuje nadzór nad wykonywaniem kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych, ich przechowywaniem oraz okresowym sprawdzeniem pod kątem dalszej przydatności do odtwarzania danych osobowych w przypadku awarii systemu informatycznego,
   8) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych oraz zapewnieniu bezpiecznej wymiany danych osobowych w sieci wewnętrznej,

9) wyjaśnia wszelkie zgłoszone nieprawidłowości i incydenty dotyczące przetwarzania danych z wykorzystaniem środków informatycznych oraz eliminuje skutki ich wystąpienia.

2. W celu prawidłowego wykonywania zadań, o których mowa w ust. 1, Administrator danych jest uprawniony do:
   1) dokonywania przeglądów, konserwacji oraz uaktualniania systemów, programów, narzędzi programowych służących do przetwarzania danych osobowych,
   2) sprawowania kontroli bezpieczeństwa w sieci komputerowej,
   3) nadawania, zmiany lub pozbawiania użytkowników uprawnień dostępu do systemu informatycznego,
   4) wykonywania polityki ochrony antywirusowej,
   5) wykonywania kopii zapasowych.

ROZDZIAŁ IV
PRAWA I OBOWIĄZKI PRACOWNIKÓW I INNYCH CZŁONKÓW PERSONELU ADMINISTRATORA DANY OSOBOWYCH

§ 15

Każdy pracownik lub inny członek personelu Administratora Danych uprawniony jest do przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie w nadanym mu upoważnieniu i tylko w celu wykonywania powierzonych mu obowiązków.

§ 16

1. Osoba, o której mowa w § 15 *Polityki Bezpieczeństwa,* jest w szczególności zobowiązana do:
   1) zachowania w tajemnicy przetwarzanych danych osobowych oraz stosowanych przez Administratora Danych środków bezpieczeństwa, w szczególności sposobów zabezpieczenia danych osobowych i złożenia w zakresie przestrzegania tego zobowiązania oświadczenia na piśmie,
   2) odpowiedniego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem zasad ochrony danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
   3) zobowiązana jest do zapoznania się z przepisami prawa w zakresie zasad ochrony danych osobowych, w tym zasadami przyjętymi w ramach *Polityki Bezpieczeństwa* oraz *Instrukcji zarządzania systemem informatycznym.*
2. W celu zapewnienia bezpieczeństwa danych osobowych, każdy pracownik lub inny członek personelu Administratora Danych, który został upoważniony do przetwarzania danych zobowiązany jest do:
   1) stosowania się do zaleceń, wytycznych i instrukcji Administratora Danych w przedmiocie przetwarzania danych osobowych,
   2) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarza się dane osobowe pod nieobecność osoby upoważnionej do przetwarzania danych,
   3) nieużywania powtórnego jednostronnie zadrukowanych dokumentów, na których znajdują się dane osobowe, zaś w przypadku ustania ich przydatności niezwłocznego ich usuwania przy użyciu niszczarki lub w inny sposób skutkujący trwałym usunięciem danych,
   4) usuwania przy użyciu niszczarki wszelkich wydruków zawierających dane osobowe, które nie będą wykorzystywane w pracy, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy,
   5) wylogowania z systemu informatycznego, schowania do szaf zamykanych na klucz wszelkich akt, dokumentów i wydruków zawierających dane osobowe lub do zamykanych szaf, gdy

pomieszczenie jest zamykane na klucz, przed opuszczeniem stanowiska pracy po zakończeniu dnia pracy,

6) zamykanie okien i drzwi w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy, a także w przypadku opadów lub innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych, z zastosowaniem wszelkich dostępnych rozwiązań technicznych,
7) korzystania z systemów informatycznych, w tym urządzeń elektronicznych, komputerów, laptopów, telefonów, tabletów, telefonów komórkowych, programów lub aplikacji komputerowych oraz zewnętrznych nośników danych w sposób zapewniający bezpieczeństwo przetwarzania danych osobowych,

3. W celu zapewnienia bezpieczeństwa danych osobowych zabrania się pracownikom i innym członkom personelu Administratora Danych, upoważnionych do przetwarzania danych osobowych:
   1) tymczasowego pozostawiania swojego miejsca pracy bez nadzoru,
   2) przekazywania innym osobom, w tym innym pracownikom oraz członkom personelu własnego identyfikatora lub hasła do konta w systemie informatycznym,
   3) korzystania z prywatnej poczty elektronicznej w celach służbowych, w szczególności przesyłania dokumentów elektronicznych i innych plików, w tym tych zawierających dane osobowe ze służbowego komputera lub serwera na prywatną pocztę elektroniczną,
   4) korzystania ze służbowej poczty elektronicznej w celach prywatnych,
   5) nieograniczonego korzystania z Internetu w celach prywatnych, w tym w szczególności pobierania plików, które nie służą celom służbowym i mogą stanowić zagrożenie dla systemu informatycznego,
   6) korzystania na służbowych komputerach z prywatnych zewnętrznych nośników danych (np. pendrive, dysk zewnętrzny, płyty CD i DVD), zarówno w celach prywatnych jak i służbowych, chyba że służą celom związanych z działalnością Administratora Danych.

§ 17

Pracownik lub inny członek personelu Administratora Danych, który w ramach wykonywania obowiązków służbowych nie przetwarza danych osobowych, a posiada wiedzę o środkach bezpieczeństwa stosowanych w ramach działalności Administratora Danych, w szczególności o sposobach zabezpieczenia, bądź ma inną wiedzę na temat danych osobowych przetwarzanych przez Administratora danych, zobowiązany jest do zachowania ich w tajemnicy i złożenia w tym zakresie oświadczenia na piśmie, zgodnie z *Załącznikiem nr 4* do *Polityki Bezpieczeństwa*.

ROZDZIAŁ V
OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

§ 18

1. Obszar, w którym przetwarzane są dane osobowe przez Administratora danych obejmuje pomieszczenia biurowe zlokalizowane w Reńskiej Wsi przy ul. Fabrycznej 1.
2. Dodatkowo obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz nośniki danych znajdujące się poza obszarem wskazanym powyżej.

§ 19

Przetwarzanie danych osobowych przez osoby upoważnione odbywa się w wyznaczonych pomieszczeniach, w godzinach pracy lub po godzinach, po uprzednim uzyskaniu zgody Administratora Danych. Wykorzystywanie akt i dokumentów, zawierających dane osobowe do pracy w domu jest

możliwe tylko po uzyskaniu upoważnienia na piśmie, udzielanego przez Administratora Danych lub osobę przez niego upoważnioną. Pracownik lub inny członek personelu Administratora Danych jest zobowiązany do zapewnienia bezpieczeństwa tych danych.

§ 20

1. Administrator Danych gwarantuje w ramach obszarów przetwarzania danych osobowych, o których mowa w § 18 *Polityki Bezpieczeństwa,* warunki zabezpieczające dane osobowe, w tym przede wszystkim ochronę danych osobowych przed osobami postronnymi.
2. W ramach obszaru, o którym mowa w § 18 ust. 1 *Polityki Bezpieczeństwa,* wydziela się strefę dostępną wyłącznie dla pracowników i pozostałych członków personelu Administratora Danych, którzy zostali upoważnieni do przetwarzania danych osobowych, oraz strefę dla pozostałych osób nieupoważnionych, w tym pozostałych pracowników i członków personelu Administratora Danych oraz jego kontrahentów.
3. Zastrzega się dostęp po godzinach pracy do strefy dostępnej wyłącznie dla pracowników i pozostałych członków personelu Administratora Danych, którzy zostali upoważnieni do przetwarzania danych osobowych, dla osób sprzątających z upoważnienia Administratora Danych oraz pozostałych przedstawicieli usług serwisowych. Administrator Danych może określić pomieszczenia, do których dostęp osób sprzątających oraz pozostałych przedstawicieli usług serwisowych będzie ograniczony i możliwy tylko pod nadzorem osób uprawnionych do przebywania w tych pomieszczaniach.

ROZDZIAŁ VI
POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH ORAZ UDOSTĘPNIENIE DANYCH OSOBOWYCH PODMIOTOWI ZEWNĘTRZNEMU

§ 21

1. Administrator Danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi, zwłaszcza w przypadkach konieczności ich wykorzystania w celach rachunkowych, księgowych, podatkowych, prawnych, administracyjnych i archiwizacyjnych.
2. Administrator Danych zobowiązuje się korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi zasad ochrony danych osobowych.

§ 22

1. Powierzenie przetwarzania danych osobowych następuje na podstawie postanowień umowy powierzenia zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej.
2. Umowa, o której mowa w ust. 1, określa w szczególności przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy (administratora i procesowa).
3. Administrator Danych prowadzi rejestr powierzeń danych osobowych, zawierający wykaz zbiorów danych oraz podmiotów, którym dane osobowe zostały powierzone do przetwarzania. Wzór rejestru określa *Załącznik nr 6* do *Polityki Bezpieczeństwa.*

§ 23

1. Podmiot, któremu powierzono przetwarzanie danych osobowych zobowiązany jest w szczególności do:

1) przetwarzania powierzonych mu danych wyłącznie w zakresie i celu, które zostały określone w zawartej z nim umowie, jak również do zachowania w tajemnicy danych osobowych powierzonych mu do przetwarzania,
2) stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności poprzez zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem zasad ochrony danych osobowych,
3) opracowania i wdrożenia do stosowania dokumentacji dotyczącej przetwarzania danych osobowych w postaci polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) zapewnienia, aby do przetwarzania danych osobowych dopuszczone były wyłącznie osoby posiadające nadane przez niego upoważnienia,
5) prowadzenia ewidencji oraz osób upoważnionych do przetwarzania danych osobowych,
6) zapewniania kontroli nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
7) zobowiązanie osób, które zostały upoważnione do przetwarzania danych osobowych do zachowania w tajemnicy tych danych osobowych oraz sposobów i zabezpieczenia,
8) niezwłocznego poinformowania Administratora Danych o sytuacji podpowierzenia danych osobowych oraz wskazania w umowie nazwy podmiotu wraz z danymi teleadresowymi, któremu zostaną podpowierzone dane osobowe.

2. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy i inni członkowie personelu podmiotu przetwarzającego w zakresie adekwatnym do celu powierzenia. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych) wymagana jest szczególna zgoda Administratora Danych na przekazanie powierzonych danych, wyrażona w formie pisemnej lub równoważnej jej formie elektronicznej.

§ 24

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu, w tym w szczególności organom wymiaru sprawiedliwości i ściągania, takim jak sąd, policja i prokuratura, może nastąpić wyłącznie w sytuacji, w której Administrator Danych udostępniający dane oraz administrator danych pozyskujących dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie wyżej wymienionej czynności.
2. Administrator Danych może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania podmiotu wnioskującego o udostępnienia danych.
3. W przypadku udostępnienia dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.
4. Administrator Danych prowadzi rejestr udostępnień danych osobowych innym osobom, zawierający wykaz zbiorów danych oraz podmiotów, którym dane osobowe zostały udostępnione. Wzór rejestru określa *Załącznik nr 6* do *Polityki Bezpieczeństwa.*

ROZDZIAŁ VII
ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 25

W celu zapewnienia należytej ochrony przetwarzania danych osobowych, w miejscu o którym mowa w § 18 *Polityki Bezpieczeństwa,* zastosowano środki zabezpieczające poddane przetwarzaniu zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych.

§ 26

1. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w odpowiednio zabezpieczonych pomieszczeniach przed dostępem i działalnością osób postronnych (zamki na klucz, karty zbliżeniowe).
2. Pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczone przed skutkami pożaru za pomocą instalacji przeciwpożarowej, w tym w szczególności systemu gaśniczego.
3. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce lub w inny sposób skutkujący trwałym usunięciem danych.

§ 27

Stosowane przez Administratora Danych zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej, dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych, a także zabezpieczenia techniczne i programowe dla procedur, aplikacji, programów, baz danych i innych narzędzi przetwarzających dane osobowe opisane zostały w *Instrukcji zarządzania systemem informatycznym*.

§ 28

1. Opracowano i wdrożono Politykę Bezpieczeństwa Informacji oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ramach działalności Administratora Danych.
2. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych oraz które podpisały oświadczenie o zachowaniu poufności zobowiązujące je do zachowania przetwarzanych danych w poufności. Dostęp osób nieposiadających stosownych upoważnień do pomieszczeń, w których przetwarzane są dane osobowe odbywa się wyłącznie za zgodą Administratora Danych lub w obecności i pod nadzorem osób upoważnionych. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3. Wszyscy pracownicy i pozostali członkowie personelu Administratora Danych posiadający dostęp do danych osobowych przed przystąpieniem do pracy są zobowiązani do zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych oraz obowiązujących procedur wewnętrznych, w tym *Polityki Bezpieczeństwa* i *Instrukcji zarządzania system informatycznym.*
4. Przetwarzanie danych dokonywane jest w warunkach zabezpieczających dane osobowe przed dostępem osób nieuprawnionych. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych osobowych.
5. Współpracując z podwykonawcami lub innym podmiotami przetwarzającymi dane osobowe stosuje się pisemne umowy powierzenia przetwarzania danych osobowych.

6. Przeprowadza się regularne przeglądy *Polityki Bezpieczeństwa* oraz *Instrukcji zarządzania systemem informatycznym*.

ROZDZIAŁ VIII
PROCDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 29

1. Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych osobowych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek systemu informatycznego, a w szczególności:
   1) nieautoryzowany dostęp do danych osobowych,
   2) utrata nośników zawierających dane osobowe,
   3) nieautoryzowane modyfikacje lub zniszczenia danych osobowych,
   4) udostępnianie danych osobowych nieautoryzowanym podmiotom,
   5) nielegalne ujawnienie danych osobowych,
   6) pozyskiwanie danych osobowych z nielegalnych źródeł.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   1) próby naruszenia danych osobowych:
      a) z zewnątrz – włamania do systemu, podsłuch, kradzież danych,
      b) z wewnątrz – nieumyślna lub celowa modyfikacja danych, kradzież danych,
   2) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne,
   3) awarie sprzętu lub uszkodzenia oprogramowania,
   4) zabór sprzętu lub nośników z ważnymi danymi,
   5) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
   6) usiłowanie zakłócenia działania systemu informatycznego.
3. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu informatycznego i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników, takich jak niewłaściwa ochrona haseł, niezamykanie pomieszczeń, szafek, okien i drzwi,
   4) zdarzenie losowe zewnętrzne, takie jak pożar, zalanie, utrata zasilania czy łączności,
   5) zdarzenie losowe wewnętrzne, takie jak awarie serwera, komputerów, twardych dysków, oprogramowania,
   6) umyślne incydenty, takie jak włamania do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadomie zniszczenie dokumentów lub danych, działanie wirusów i innego szkodliwego oprogramowania.
4. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach bezpieczeństwa danych osobowych zalicza się:
   1) zgłoszenia od użytkowników, pracowników lub innych członków personelu Administratora Danych,
   2) alarmy z systemów informatycznych,
   3) analizy incydentów,
   4) wyniki audytów i kontroli.

§ 30

1. W przypadku stwierdzenia naruszenia bezpieczeństwa ochrony danych osobowych, każdy pracownik lub pozostały członek personelu Administratora Danych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie Administratora Danych oraz bezpośredniego przełożonego, a następnie stosować się do podjętych przez niego decyzji.
2. Powiadomienie, o naruszeniu bezpieczeństwa danych osobowych powinno zawierać:
   1) opis stwierdzonego naruszenia ochrony danych osobowych,
   2) określenie sytuacji, miejsca i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
   3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia,
   4) określenie znanych danej osobie sposobów zabezpieczenia bezpieczeństwa danych osobowych oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 31

1. W przypadku stwierdzenia wystąpienia zagrożenia Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego ustala zakres i przyczyny zagrożenia oraz jego potencjalne skutki, inicjuje ewentualne działania dyscyplinarne, rekomenduje działania prewencyjne zmierzające do eliminacji podobnych zagrożeń w przyszłości oraz dokumentuje prowadzone postępowanie.
2. W przypadku stwierdzenia naruszenia Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki, wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze poprzez usunięcia skutków incydentu oraz ograniczenie szkody,
   2) ustala osoby odpowiedzialne za naruszenia,
   3) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   4) dokumentuje prowadzone postępowanie.
3. Administrator Danych jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabość systemu ochrony danych osobowych. Gdy stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych określa źródło powstania incydentu zagrożenia lub słabości, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę za nią odpowiedzialną.
4. Administrator Danych jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.
5. Administrator Danych prowadzi rejestr incydentów i zagrożeń. Wzór rejestru określony został w *Załączniku nr 7* do *Polityki Bezpieczeństwa.*

§ 32

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli jest to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

§ 33

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z obowiązujących przepisów prawa.
2. Niezależnie od odpowiedzialności, o której mowa w ust. 1, łamanie zasad wynikających z niniejszej *Polityki Bezpieczeństwa* może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych i może skutkować nałożeniem kar porządkowych na zasadach określonych w przepisach prawa pracy oraz procedurach wewnętrznych, w szczególności w przypadku osoby która po stwierdzeniu naruszenia bezpieczeństwa danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie Administratora Danych.
3. Udokumentowane umyślne złamanie zasad określonych w niniejszej Polityce Bezpieczeństwa jest traktowane jako ciężkie naruszenie obowiązków pracowniczych uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia z winy pracownika.
4. Jeśli skutkiem działania lub zaniechania, o których mowa w ust. 2 i 3 jest pracownik to ponosi on odpowiedzialność materialną na zasadach określonych w przepisach prawa pracy.
5. Jeśli skutkiem działania lub zaniechania, o których mowa w ust. 2 i 3 jest inny członek personelu Administratora Danych to ponosi on odpowiedzialność na zasadach ogólnych określonych w przepisach prawa cywilnego.

ROZDZIAŁ IX
POSTANOWIENIA KOŃCOWE

§ 34

Dopuszcza się odstępstwa od dokumentów wzorcowych wskazanych w ramach *załączników 2, 3a, 3b, 3c, 3d, 4, 5, 6, 7* do *Polityki Bezpieczeństwa* z zastrzeżeniem zachowania zgodności ich treści z obowiązującymi przepisami prawa

§ 35

1. *Polityka Bezpieczeństwa* wraz załącznikami podlega przeglądowi w zakresie jej postanowień co najmniej raz na rok.
2. W razie istotnych zmian dotyczących przetwarzania danych osobowych Administrator Danych może zarządzić przegląd *Polityki Bezpieczeństwa* wraz z *Załącznikami* stosownie do potrzeb.
3. W ramach przeglądu, o którym mowa w ust. 1, Administrator Danych jest zobowiązany do oceny, czy *Polityka Bezpieczeństwa* i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   1) zmian w budowie systemu informatycznego,
   2) zmian organizacyjnych Administratora Danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   3) zmian w obowiązującym prawie.

§ 36

W zakresie nieuregulowanym postanowieniami *Polityki Bezpieczeństwa* zastosowanie mają przepisy prawa obowiązującego, w tym w szczególności przepisy o których mowa w § 1 ust. 1 *Polityki Bezpieczeństwa.*

§ 37

Niniejsza Polityka Bezpieczeństwa wchodzi w życie z 25 maja 2018 r.

Wykaz załączników:

- *Załącznik nr 1 –* „Instrukcja zarządzania system informatycznym”
- *Załącznik nr 2 –* „Wzór rejestru przetwarzania danych osobowych”
- *Załącznik nr 3a –* „Wzór zgody na przetwarzanie danych osobowych”
- *Załącznik nr 3b –* „Wzór zgody na przetwarzanie danych osobowych pracownika lub innego członka personelu w celach kadrowych”
- *Załącznik nr 3c –* „Wzór zgody na przetwarzanie danych osobowych w celu wykonywania umowy”
- *Załącznik nr 3d –* „Wzór oświadczenia o przetwarzaniu danych osobowych w celu wykonywania umowy”
- *Załącznik nr 4a -* „Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem o poufności ”
- *Załącznik nr 4b –* „Wzór protokołu usunięcia danych”
- *Załącznik nr 5 –* „Wzór wykazu osób upoważnionych do przetwarzania danych osobowych”
- *Załącznik nr 6 –* „Wzór rejestru powierzeń i udostępnień danych osobowych”
- *Załącznik nr 7 –* „Wzór rejestru incydentów i zagrożeń danych osobowych”

INSTRUKACJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

ROZDZIAŁ I
POSTANOWIENIA OGÓLNE

§ 1

1. *Instrukcja zarządzania systemem informatycznym* służącym do przetwarzania danych osobowych, zwana dalej *Instrukcją*, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych działalności gospodarczej MIETEX Sp. z o.o., 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: *Rozporządzenie RODO*.
2. *Instrukcja* jest dokumentem, który określa zasady i sposób postępowania pracowników i pozostałych członków personelu działalności gospodarczej MIETEX Sp. z o.o. w związku z przetwarzaniem danych osobowych w systemach informatycznych.
3. Celem *Instrukcji* jest w szczególności określenie zasad zarządzania systemami informatycznymi służącymi w ramach działalności gospodarczej MIETEX Sp. z o.o. do przetwarzania danych osobowych oraz zapewniania odpowiedniego poziomu bezpieczeństwa i ochrony przed przetwarzaniem danych osobowych w zbiorach w sposób sprzeczny z postanowieniami obowiązujących przepisów prawa, *Polityki Bezpieczeństwa Informacji* oraz stosownych umów powierzenia przetwarzania danych osobowych.

ROZDZIAŁ II
PROCEDURY NADAWANIA, AKTUALIZOWANIA I WYCOFYWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH ORAZ REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

§ 2

Za bezpieczeństwo danych osobowych w systemie informatycznym dostępnym w ramach działalności gospodarczej MIETEX Sp. z o.o. i za właściwy nadzór odpowiedzialny jest Administrator Danych Mieczysław Matyjewicz.

§ 3

1. 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, które stanowi *Załącznik nr 4a* do *Polityki Bezpieczeństwa.*
2. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany identyfikator użytkownika. Dla wszystkich użytkowników

stosowane są uprawnienia do zasobów i zbiorów według zasady niezbędnego minimum potrzebnego do pracy.
3. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

§ 4

Osoby upoważnione do przetwarzania danych osobowych powinny wykonywać powierzone im czynności na kontach zwykłych użytkowników. Praca na kontach administracyjnych jest dopuszczalna tylko dla upoważnionych przez Administratora Danych osób.

§ 5

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania danych i środków zabezpieczenia w tajemnicy.
2. Obowiązek, o którym mowa w ust. 1, istnieje również po ustaniu zatrudnienia lub współpracy z Administratorem Danych.

§ 6

1. Administrator Danych jest odpowiedzialny za aktualizację i wycofywanie uprawnień dostępu do systemów informatycznych.
2. Administrator Danych, w celu realizacji obowiązku, o którym mowa w ust. 1, prowadzi przegląd aktualności kont użytkowników wraz z nadanymi im uprawnieniami.

§ 7

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.

ROZDZIAŁ III
METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

§ 8

1. W systemie informatycznym stosuje się uwierzytelnianie na poziomie dostępu do systemu operacyjnego.
2. Do uwierzytelnienia użytkownika na poziomie dostępu do systemu operacyjnego stosuje się hasło oraz identyfikator użytkownika.

§ 9

1. Hasło użytkownika powinno składać się co najmniej z 8 znaków oraz zawierać w razie możliwości małe i wielkie litery, a także cyfry oraz znaki specjalne. Hasło nie powinno być identyczne z identyfikatorem użytkownika ani z jego imieniem i nazwiskiem. Zabrania się używania hasła lub identyfikatora innego użytkownika.
2. Hasło użytkownika podlega okresowej zmianie nie rzadziej niż co 90 dni.
3. W przypadku podejrzenia, że hasło mogło zostać ujawnione należy zmienić je niezwłocznie.

§ 10

1. Użytkownik bezwzględnie nie może ujawnić osobom trzecim środków uwierzytelniania, w tym identyfikatora oraz jakichkolwiek – aktualnych, poprzednich lub tymczasowych haseł mu powierzonych.
2. Hasła użytkowników umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.

§ 11

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu,
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   3) informacji o odbiorcach, którym Dane osobowe zostały udostępnione.
2. W przypadku braku funkcjonalności, o której mowa w ust. 1 rejestr informacji jest prowadzony w formie pisemnej.

ROZDZIAŁ IV
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 12

1. Rejestrowanie użytkownika odbywa się z chwilą rozpoczęcia przez niego pracy w systemie.
2. Procedura, o której mowa w ust. 1 rozpoczyna się od wprowadzenia identyfikatora oraz hasła. Na tej podstawie system stwierdza tożsamość i przydziela uprawnienia użytkownika.
3. Po poprawnym wykonaniu czynności, o której mowa w ust. 2 użytkownik może wykonywać wszystkie czynności w ramach przyznanych mu uprawnień.

§ 13

1. Procedura uwierzytelniania, o której mowa w § 12 *Instrukcji* powinna być wykonana przez użytkownika w sposób uniemożliwiający zapoznanie się z hasłem i identyfikatorem osobom postronnym, tzn. nikt poza użytkownikiem nie powinien widzieć ekranu monitora oraz klawiatury w trakcie wprowadzania danych uwierzytelniających.
2. W przypadku braku możliwości bezpiecznego zalogowania lub problemów z funkcjonowaniem systemu, użytkownik zobowiązany jest do przerwania czynności i powrócenia do niej w warunkach bezpiecznych.

§ 14

1. Należy zwrócić szczególną uwagę na otoczenie, w jakim znajduje się stanowisko komputerowe. Niedopuszczalne jest umieszczenie przedmiotów, które mogłyby uszkodzić sprzęt komputerowy.
2. Należy dbać o to, aby stanowisko komputerowe było zadbane i utrzymane w czystości. Zabrania się spożywania pokarmów i płynów w bezpośrednim otoczeniu stanowiska komputerowego, które skutkowałoby jego uszkodzeniem, np. zalaniem klawiatury.

§ 15

1. W przypadku opuszczenia stanowiska pracy użytkownik zobowiązany jest aktywować wygaszacz ekranu lub zablokować w inny sposób stację roboczą.

2. Zawieszenie pracy w systemie wymaga od użytkownika wylogowania się i zakończenia pracy w systemie. Każda następna operacja w systemie musi być ponownie oparta na wykonaniu procedury uwierzytelniania użytkownika.
3. Po zakończeniu pracy użytkownik wyloguje się z systemu, w tym poprzez wyłączenie stacji roboczej.

ROZDZIAŁ V
PROCEDURY KORZYSTANIA Z OPROGRAMOWANIA

§ 16

1. Można korzystać wyłącznie z oprogramowania i systemów dopuszczonych przez Administratora Danych do eksploatacji.
2. W szczególnych sytuacjach dopuszczone jest stosowania lub wprowadzenie do systemu informatycznego aplikacji trzecich pod warunkiem przestrzegania warunków umowy licencyjnej oraz uzyskania zgody Administratora Danych.
3. Każda instalacja bądź uruchomienie nowego oprogramowania musi być poprzedzone kontrolą antywirusową pakietu instalacyjnego.

§ 17

1. Zabronione jest użytkowanie oprogramowania niezwiązanego z zakresem wykonywanych obowiązków służbowych użytkownika systemu informatycznego.
2. Zabrania się korzystania z programów i systemów niebędących własnością Administratora Danych lub niedopuszczonych przez niego do użytkowania. Dotyczy to w szczególności:
   1) nielegalnego oprogramowania naruszającego prawa autorskie,
   2) legalnego oprogramowania nieposiadającego ważnej licencji.

§ 18

1. Administrator Danych zobowiązany jest do nadzorowania zgodności instalowanego oprogramowania z posiadanymi licencjami.
2. Dopuszcza się możliwość monitorowania jednostek komputerowych pod kątem zainstalowanego oprogramowania oraz przechowywanych lokalnie plików.

ROZDZIAŁ VI
PROCEDURY KORZYSTANIA Z INTERNETU I POCZTY ELEKTRONICZNEJ

§ 19

Każdy z użytkowników jest zobowiązany do korzystania z Internetu i poczty elektronicznej w sposób gwarantujący bezpieczeństwo danych przesyłanych przez te media.

§ 20

1. Zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych niezwiązanych w wykonywaniem obowiązków pracowniczych. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane.

2. Do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez Administratora Danych formy dostępu.
3. Administrator Danych osobowych może stosować mechanizmy monitorujące przeglądanie Internetu przez użytkowników w graniach poszanowania jego prawa do godności oraz prywatności, w tym w szczególności:
   1) blokować strony internetowe określonego typu,
   2) blokowanie określone strony internetowe.

§ 21

Użytkownicy poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:
1) do wymiany korespondencji w czasie korzystania z systemu informatycznego jest wykorzystywana tylko służbowa poczta elektroniczna,
2) przesyłanie informacji za pośrednictwem poczty elektronicznej powinno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych,
3) w przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Danych,
4) użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu,
5) w przypadku przesyłania danych wrażliwych lub informacji stanowiących tajemnicę służbową należy wykorzystywać mechanizmy kryptograficzne,
6) jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją,
7) użytkownicy nie powinni otwierać przesyłek mailowych od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki użytkownik powinien ją zniszczyć lub skontaktować się z Administratorem Danych,
8) użytkownicy nie mogą uruchamiać nieznanych sobie załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu Administratora Danych, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji,
9) użytkownicy nie mogą rozsyłać za pośrednictwem poczty elektronicznej informacji, które mogą mieć wpływ na bezpieczeństwa i stabilność systemu informatycznego.

ROZDZIAŁ VII
KOPIE ZAPASOWE ZBIORÓW DANYCH

§ 22

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Administratora Danych.
2. Odpowiedzialnym za nadzór nad tworzeniem kopii zapasowych danych osobowych oraz narzędzi programowych służących do przetwarzania danych jest Administrator Danych.

§ 23

1. Do archiwizacji danych służą trwałe cyfrowe nośniki danych, takie jak płyta CD/DVD, pamięć trwała, dysk zdalny.

2. Zaleca się dokonywanie kopii danych minimum raz w miesiącu.

§ 24

1. Kopie zapasowe powinny być przechowywane w lokalizacji innych niż lokalizacja oryginalnych danych, zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
2. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.

ROZDZIAŁ VIII
ZASADY BEZPIECZNEGO PRZECHOWYWANIA, TRANSPORTU I NISZCZENIA URZĄDZEŃ ORAZ INNYCH ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§ 25

Dane osobowe znajdujące się na komputerach przenośnych są zabezpieczone poprzez szyfrowanie całej powierzchni dysków twardych.

§ 26

1. Dane osobiste zapisane na dyskach zewnętrznych lub innych nośnikach informacji, po ustaniu potrzeby ich przechowywania, należy niezwłocznie usunąć z urządzenia oraz wykonać formatowanie nośnika.
2. W przypadku, kiedy nośnik pozwala jedynie na jednokrotny zapis należy go zniszczyć.
3. Zniszczenie nośnika informacji, który zawierał kiedykolwiek dane osobiste odbywa się pod nadzorem Administratora Danych z wykorzystaniem urządzeń przystosowanych do tego rodzaju czynności oraz zostaje odnotowane w rejestrze utylizacji, który prowadzi Administrator Danych.

§ 27

1. Transport urządzeń, dysków i innych nośników informacji poza obszar przetwarzania danych jest dozwolony jedynie za zgodą Administratora Danych.
2. Osoba wynosząca urządzenie. dysk lub inny nośnik informacji poza obszar przetwarzania danych zobowiązana jest do zachowania szczególnych środków bezpieczeństwa w celu zapobieżenia dostępowi do nośnika osobom nieupoważnionym. W szczególności niedozwolone jest pozostawienie nośnika poza obszarem przetwarzania danych bez nadzoru.

ROZDZIAŁ IX
SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST NARUSZENIE BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO, W TYM UZYSKANIE DO NIEGO NIEUPRAWNIONEGO DOSTĘPU

§ 28

1. Ze względu na podłączenie systemu informatycznego Administratora Danych do sieci publicznej wszystkie jego elementy są narażone na ingerencję szkodliwego oprogramowania.
2. Źródłami zagrożeń dla systemu informatycznego są zewnętrzne działania osób trzecich, które poprzez sieć publiczną próbują uzyskać nieuprawniony dostęp do zasobów informatycznych Administratora Danych lub działania mające na celu zainfekowanie systemu wirusem komputerowym oraz wewnętrzne działania pracowników lub pozostałego personelu Administratora Danych, w tym próby instalacji nielicencjonowanego oprogramowania lub użycie zainfekowanych wirusem nośników informacji w komputerach służbowych.

§ 29

System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje system antywirusowy, blokadę firewall oraz szyfrowanie nośników danych.

§ 30

1. Sprawdzenie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się za pomocą licencjonowanego oprogramowania.
2. Użytkowany system jest automatycznie skanowany ze stale zdefiniowaną częstotliwością.
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy:
   1) uruchomić program antywirusowy i skontrolować użytkowany system,
   2) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.
5. Jeżeli operacja usunięcia wirusa, o której mowa w ust. 4, się nie powiedzie, należy:
   1) zakończyć pracę w systemie komputerowym,
   2) odłączyć zainfekowany komputer od sieci,
   3) powiadomić o zaistniałej sytuacji Administratora Danych.

§ 31

Przyłączając do komputerów zewnętrzne nośniki (np.: pendrive, zewnętrzny dysk itp.) należy go każdorazowo automatycznie zeskanować pod kątem ewentualnych zagrożeń.

ROZDZIAŁ X
PROCEDURY WYKONYWANIA NAPRAW, PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFOMATYCZNEGO ORAZ ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI SŁJUŻACYCH DO PRZETWARZANIA DANYCH

§ 32

1. Celem wykonywania okresowych przeglądów systemu informatycznego jest określenie wymaganego przepisami prawa poziomu zabezpieczeń przetwarzania danych osobowych.
2. Przegląd zgodności z zasadami bezpieczeństwa zasobów teleinformatycznych oraz urządzeń infrastruktury teleinformatycznej należy przeprowadzać przynajmniej raz na rok.

§ 33

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
   1) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do przetwarzania danych,
   2) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
   3) przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

§ 34

1. W przypadku likwidacji sprzętu informatycznego lub nośników danych należy każdorazowo sporządzić protokół z czynności.
2. W przypadku powierzenia naprawy lub likwidacji dysków lub innych nośników informacji zawierających dane osobowe podmiotowi nieposiadającemu upoważnienia do przetwarzania danych osobowych należy:
   1) w przypadku likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe uszkadza się nośnik w sposób uniemożliwiający ich odczytanie i odzyskanie;
   2) w przypadku naprawy - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem Administratora Danych.

Załącznik nr 2

Wzór rejestru przetwarzania danych osobowych

REJESTR PRZETWARZANIA DANYCH OSOBOWYCH

Nazwa oraz dane kontaktowe Administratora Danych	
Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	
Cele przetwarzania danych osobowych	
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
Informacja o przekazywaniu danych osobowych do państwa trzeciego	
Planowane terminy usunięcia poszczególnych kategorii danych	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	

Załącznik nr 3a

Wzór zgody na przetwarzanie danych osobowych

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Ja, niżej podpisany, …….. wyrażam zgodę na przetwarzanie moich danych osobowych zebranych w ramach działalności gospodarczej MIETEX Sp. z o.o. w celach ……., w tym w szczególności:

1) …..,
2) …..

Jednocześnie wyrażam zgodę na dalsze przekazywanie moich danych osobowych podmiotom trzecim, zwłaszcza usługodawcom z zakresu ……, w zakresie niezbędnym do realizacji obowiązków ustawowych oraz wykonywania prawnie uzasadnionych interesów realizowanych w ramach działalności gospodarczej MIETEX Sp. z o.o..

_____

data i miejsce wyrażenia zgody, podpis

MIECZYSŁAW MATYJEWICZ, prowadzący działalność gospodarczą pod nazwą MIETEX Sp. z o.o., ul. Fabryczna 1, 47-208 Reńska Wieś, NIP 7492114930, REGON 523259581, jako Administrator Danych, informuje że:

1) podanie danych jest niezbędne w celu ……..,
   w tym ……,
   brak zgody na przetwarzanie danych skutkuje ……
2) zebrane dane będą przetwarzane przez Administratora Danych na podstawie art. 6 ust. 1 lit ……. *Rozporządzenia RODO,*
3) Administrator Danych Osobowych powierza dalsze przetwarzanie danych następującym podmiotom trzecim: …….., w zakresie ……,
4) umożliwia się dostęp do treści zebranych na swój temat danych i ich sprostowania, usunięcia, ograniczenia przetwarzania, zapewnia prawo do przenoszenia danych, prawo do cofnięcie zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, z zastrzeżeniem przetwarzania danych w zakresie wymaganym przez przepisy prawa,
5) Administrator Danych nie ma obowiązku powołania inspektora ochrony danych osobowych,
6) Administrator Danych nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej, ani innym podmiotom trzecim, za wyjątkiem organów upoważnionych na podstawie przepisów prawa,
7) dane osobowe będą przechowywane przez okres …..……,
8) przetwarzane dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym decyzji będącej wynikiem profilowania,
9) osoba, której dane dotyczą ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku gdy uzna, że przetwarzanie danych osobowych jej dotyczących naruszenia zasady ochrony danych osobowych.

Załącznik nr 3b

Wzór zgody na przetwarzanie danych osobowych pracownika lub innego członka personelu w celach kadrowych

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH
W CELACH KADROWYCH

Ja, niżej podpisany, …….. wyrażam zgodę na przetwarzanie moich danych osobowych zebranych i przetwarzanych w ramach działalności gospodarczej MIETEX Sp. z o.o. w celach prowadzenia polityki kadrowo-płacowej oraz socjalnej, w tym w szczególności:

1) informacji zawartych w aktach osobowych pracownika i innych dokumentach pracowniczych,
2) danych zawartych w programie kadrowym lub płacowym,
3) uzyskania świadczeń socjalnych na rzecz pracowników.

Jednocześnie wyrażam zgodę na dalsze przekazywanie moich danych osobowych podmiotom trzecim, zwłaszcza usługodawcom z zakresu księgowości oraz usług prawnych, w zakresie niezbędnym do realizacji obowiązków ustawowych oraz wykonywania prawnie uzasadnionych interesów realizowanych w ramach działalności gospodarczej MIETEX Sp. z o.o..

_____

data i miejsce wyrażenia zgody, podpis

MIECZYSŁAW MATYJEWICZ, prowadzący działalność gospodarczą pod nazwą MIETEX Sp. z o.o., ul. Fabryczna 1, 47-208 Reńska Wieś, NIP 7492114930, REGON 523259581, jako Administrator Danych, informuje że:

1) podanie danych jest niezbędne w celu realizacji praw i obowiązków pracodawcy oraz pracownika, a także Agencji Pracy Tymczasowych, w tym prowadzenia właściwej polityki kadrowo-płacowej Administratora Danych, brak zgody na przetwarzanie danych uniemożliwia realizację praw i obowiązków pracodawcy wynikających ze stosunku pracy, wobec czego skutkuje odmową zawarcia stosunku pracy lub rozwiązania stosunku pracy już istniejącego,
2) zebrane dane będą przetwarzane przez Administratora Danych na podstawie art. 6 ust. 1 lit a, b, c, f *Rozporządzenia RODO,*
3) Administrator Danych powierza dalsze przetwarzanie danych podmiotom trzecim, zwłaszcza usługodawcom z zakresu księgowości oraz usług prawnych, wyłącznie w zakresie niezbędnym do realizacji obowiązków ustawowych oraz niezbędnych do wykonywania praw w ramach działalności gospodarczej MIETEX Sp. z o.o.,
4) umożliwia się dostęp do treści zebranych na swój temat danych i ich sprostowania, usunięcia, ograniczenia przetwarzania, zapewnia prawo do przenoszenia danych, prawo do cofnięcie zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, z zastrzeżeniem przetwarzania danych w zakresie wymaganym przez przepisy prawa,
5) Administrator Danych nie ma obowiązku powołania inspektora ochrony danych osobowych,
6) Administrator Danych nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej, ani innym podmiotom trzecim, za wyjątkiem organów upoważnionych na podstawie przepisów prawa,
7) dane osobowe będą przechowywane przez okres niezbędny do wykonywania umowy oraz przez czas przedawnienia wszelkich roszczeń związanych z umową,
8) przetwarzane dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym decyzji będącej wynikiem profilowania,
9) osoba, której dane dotyczą ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku gdy uzna, że przetwarzanie danych osobowych jej dotyczących naruszenia zasady ochrony danych osobowych.

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH
W CELU WYKONANIA UMOWY

Ja, niżej podpisany, …….. wyrażam zgodę na przetwarzanie moich danych osobowych zebranych i przetwarzanych w ramach działalności gospodarczej MIETEX Sp. z o.o. w celu wykonania zawartej umowy oraz w celach księgowych, w tym w szczególności następujących danych:

1) danych korespondencyjnych i teleadresowych, w tym danych dotyczących prowadzonej przeze mnie działalności gospodarczej, o ile taka jest prowadzona,
2) danych rachunkowych,
3) informacji wskazanych na dokumentach finansowych.

Jednocześnie wyrażam zgodę na dalsze przekazywanie moich danych osobowych podmiotom trzecim, zwłaszcza usługodawcą zakresu księgowości oraz usług prawnych, w zakresie niezbędnym do realizacji obowiązków ustawowych oraz wykonywania prawnie uzasadnionych interesów realizowanych w ramach działalności gospodarczej MIETEX Sp. z o.o..

_____

data i miejsce wyrażenia zgody, podpis

MIECZYSŁAW MATYJEWICZ, prowadzący działalność gospodarczą pod nazwą MIETEX Sp. z o.o., ul. Fabryczna 1, 47-208 Reńska Wieś, NIP 7492114930, REGON 523259581, jako Administrator Danych, informuje że:

1) podanie danych jest niezbędne w celu realizacji praw i obowiązków związanych z wykonaniem zawartej pomiędzy stronami umowy, w tym prowadzenia dokumentacji księgowych Administratora Danych Osobowych, brak zgody na przetwarzanie danych uniemożliwia zawarcie oraz wykonanie umowy pomiędzy stronami,
2) zebrane dane będą przetwarzane przez Administratora Danych Osobowych na podstawie art. 6 ust. 1 lit. a, b, c i f *Rozporządzenia RODO,*
3) Administrator Danych powierza dalsze przetwarzanie danych podmiotom trzecim, zwłaszcza usługodawcom z zakresu księgowości oraz usług prawnych, wyłącznie w zakresie niezbędnym do realizacji obowiązków ustawowych oraz niezbędnych do wykonywania praw w ramach działalności gospodarczej MIETEX Sp. z o.o.,
4) umożliwia się dostęp do treści zebranych na swój temat danych i ich sprostowania, usunięcia, ograniczenia przetwarzania, zapewnia prawo do przenoszenia danych, prawo do cofnięcie zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, z zastrzeżeniem przetwarzania danych w zakresie wymaganym przez przepisy prawa,
5) Administrator Danych nie ma obowiązku powołania inspektora ochrony danych osobowych,
6) Administrator Danych nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej, ani innym podmiotom trzecim, za wyjątkiem organów upoważnionych na podstawie przepisów prawa,
7) dane osobowe będą przechowywane przez okres niezbędny do wykonywania umowy oraz przez czas przedawnienia wszelkich roszczeń związanych z umową,
8) przetwarzane dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym decyzji będącej wynikiem profilowania,
9) osoba, której dane dotyczą ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku gdy uzna, że przetwarzanie danych osobowych jej dotyczących naruszenia zasady ochrony danych osobowych.

MIECZYSŁAW MATYJEWICZ, prowadzący działalność gospodarczą pod nazwą MIETEX Sp. z o.o., ul. Fabryczna 1, 47-208 Reńska Wieś, NIP 7492114930, REGON 523259581, jako Administrator Danych, informuje że w celu wykonania zawartej umowy:

1) wykorzystanie pozyskanych danych jest niezbędne w celu realizacji praw i obowiązków związanych z wykonaniem zawartej pomiędzy stronami umowy, w tym prowadzenia dokumentacji księgowych Administratora Danych Osobowych, brak zgody na przetwarzanie danych uniemożliwia zawarcie oraz wykonanie umowy pomiędzy stronami,
2) zebrane dane będą przetwarzane przez Administratora Danych Osobowych na podstawie art. 6 ust. 1 lit. a, b, c i f *Rozporządzenia RODO,*
3) Administrator Danych powierza dalsze przetwarzanie danych podmiotom trzecim, zwłaszcza usługodawcom z zakresu księgowości oraz usług prawnych, wyłącznie w zakresie niezbędnym do realizacji obowiązków ustawowych oraz niezbędnych do wykonywania praw w ramach działalności gospodarczej MIETEX Sp. z o.o.,
4) umożliwia się dostęp do treści zebranych na swój temat danych i ich sprostowania, usunięcia, ograniczenia przetwarzania, zapewnia prawo do przenoszenia danych, prawo do cofnięcie zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, z zastrzeżeniem przetwarzania danych w zakresie wymaganym przez przepisy prawa,
5) Administrator Danych nie ma obowiązku powołania inspektora ochrony danych osobowych,
6) Administrator Danych nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej, ani innym podmiotom trzecim, za wyjątkiem organów upoważnionych na podstawie przepisów prawa,
7) dane osobowe będą przechowywane przez okres niezbędny do wykonywania umowy oraz przez czas przedawnienia wszelkich roszczeń związanych z umową,
8) przetwarzane dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym decyzji będącej wynikiem profilowania,
9) osoba, której dane dotyczą ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, w przypadku gdy uzna, że przetwarzanie danych osobowych jej dotyczących naruszenia zasady ochrony danych osobowych.

Załącznik nr 4a

Wzór upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem o poufności

Reńska Wieś, dnia ……..

UPOWAŻNIENIE
do przetwarzania danych osobowych oraz obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzanych danych osobowych

Działając w imieniu własnym upoważniam Pana/ Panią ……... (*imię i nazwisko upoważnianego*) jako pracownika lub innego członka personelu działalności gospodarczej MIETEX Sp. z o.o. do przetwarzania danych osobowych w następującym zakresie:

NAZWA SYSTEMU INFORMATYCZNEGO / ZBIORU DANYCH OSOBOWYCH	ZAKRES OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH
np. zbiór danych Pracowników	*np. wgląd, wprowadzenie, modyfikacja, usuwanie, archiwizacja*

Niniejszego upoważnienia udziela się na czas zatrudnienia / współpracy upoważnionego, z zastrzeżeniem prawa do jego natychmiastowego odwołania, jako Administratora Danych.

Zobowiązuje się Pana / Panią do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wdrożonych do stosowania w ramach działalności gospodarczej MIETEX Sp. z o.o. *Polityki Bezpieczeństwa* i *Instrukcji zarządzania systemem informatycznym.*

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania w tajemnicy danych osobowych i sposób ich zabezpieczeń, również po odwołaniu upoważnienia, a także ustaniu stosunku pracy/rozwiązania umowy/zakończeniu realizacji zadań związanych z przetwarzaniem danych osobowych.

_____ _____

Administrator Danych Osoba upoważnione

Załącznik:
1) oświadczenie o poufności.

OŚWIADCZENIE O POUFNOŚCI

Ja, niżej podpisany/podpisana, …… oświadczam, że w dniu ……..……. zostałem zapoznany/zostałam zapoznana przez Mieczysława Matyjewicza, jako Administratora Danych, z przepisami dotyczącymi ochrony danych osobowych, w tym wdrożoną w ramach działalności Administratora Danych Osobowych *Polityką Bezpieczeństwa Informacji* oraz *Instrukcją zarządzania systemem informatycznym.*

Jako osoba upoważniona do przetwarzania danych osobowych zobowiązuje się do:

1) zachowania w tajemnicy danych osobowych przetwarzanych przez Administratora Danych oraz sposób ich zabezpieczenia,
2) nieujawniania danych osobowych podmiotom nieuprawnionym w jakiejkolwiek formie bez zgody Administratora Danych,
3) przestrzegania postanowień dokumentacji ochrony danych osobowych,
4) należytego zabezpieczania dokumentów papierowych przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem,
5) należytego zabezpieczenia dokumentów pomieszczeń, w którym przetwarza się dane osobowe,
6) należytej dbałości o sprzęt informatyczny oraz oprogramowanie Administratora Danych oraz korzystania z niego wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
7) wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora Danych oraz niepodejmowania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł,
8) wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą Administratora Danych Osobowych oraz zgodnie z dokumentacją ochrony danych osobowych.

Przyjmuje do wiadomości, że:

1) naruszenie przeze mnie podstawowych obowiązków umownych, w tym pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Administratora Danych jako pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą zastosowanie kary porządkowej albo wypowiedzenia przez pracodawcę umowy o pracę lub rozwiązania przez pracodawcę tejże umowy bez wypowiedzenia z winy pracownika, zgodnie z przepisami prawa pracy,
2) naruszenie zasad ochrony danych osobowych może spowodować odpowiedzialność karną na zasadach określonych w przepisach odrębnych,
3) naruszenie zasad ochrony danych osobowych może spowodować odpowiedzialność cywilnoprawną, w tym odpowiedzialność materialną, z tytułu wyrządzonej szkody według zasad określonych w przepisach odrębnych.

_____

data i miejsce złożenia oświadczenia, podpis

Załącznik nr 4b

Wzór protokołu usunięcia danych

Reńska Wieś, dnia ……..

PROTOKOŁU
usunięcia danych osobowych ze zbioru danych

1. .....
(rodzaj i nazwa zbioru danych)

2. .....
(przyczyna usunięcia danych)

3. .....
(opis usuniętych danych)

4. .....
(opis sposobu usunięcie danych)

_____
Administrator Danych

Załącznik nr 5

Wzór wykazu osób upoważnionych do przetwarzania danych osobowych

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

NR	IMIĘ I NAZWISKO OSOBY UPOWAŻNIONEJ	DATA NADANIA UPOWAŻNIENIA I JEGO NUMER	ZAKRES UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	ROZSZERZENIE / MODYFIKACJA UPOWAŻNIENIA
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18					
19.					
20.					

Załącznik nr 6

Wzór rejestru powierzeń i udostępniania danych osobowych

REJESTR POWIERZEŃ I UDOSTĘPNIEŃ DANYCH OSOBOWYCH

POWIERZENIE				
L.P	**NAZWA ZBIORU DANYCH OSOBOWYCH**	**NAZWA PROCESORA**	**UMOWA POWIERZENIA (NAZWA, DATA)**	**ZAKRES POWIERZENIA (JAKIE DANE – CAŁY ZBIÓR / NIEKTÓRE INFORMACJE)**
1.				
2.				
3.				
4.				
5.				
UDOSTĘPNIENIE				
L.P.	**NAZWA ZBIORU DANYCH OSOBOWYCH**	**NAZWA ADMINISTRATORA**	**PODSTAWA UDOSTĘPNIENIA DANYCH**	**ZAKRES UDOSTĘPNIENIA (JAKIE DANE – CAŁY ZBIÓR / NIEKTÓRE INFORMACJE)**
1.				
2.				
3.				
4.				
5.				

Załącznik nr 7

Wzór rejestru incydentów i zagrożeń danych osobowych

REJESTR INCYDENTÓW I ZAGROŻEŃ DANYCH OSOBOWYCH

KOD	DATA I GODZINA INCYDENTU	RODZAJ INCYDENTU (UCHYBIENIE/ZAGROŻENIE)	OPIS INCYDENTU	SKUTKI INCYDENTU	DZIAŁANIA NAPRAWCZE
1.					
2.					
3.					
4.					
5.					
6.					
7.					