POLITYKA BEZPIECZEŃSTWA

ADMINISTRATOR DANYCH:

MECHANIKA MASZYN „MECH-MASZ” HENRYK SZCZECIŃSKI

88-400 Żnin, Szpitalna 20 / Jaroszewo 80

Data i miejsce sporządzenia	Żnin 14.05.2018
Ilość stron	15

Spis treści:

1. Mechanika Maszyn „Mech-Masz” Henryk Szczeciński właściciel Henryki Szczeciński wdraża niniejszą Politykę Bezpieczeństwa.

Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Administratora Danych z Ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi oraz późniejszymi zmianami.

2. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
3. Na politykę Bezpieczeństwa składają się następujące informacje
   a) Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
   b) Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
   c) Opis struktury danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
   d) Sposób przepływu danych pomiędzy poszczególnymi systemami’
   e) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
4. Wyjaśnienie terminów używanych w dokumencie:
   a) **Administrator danych-**jednostka organizacyjna tj. Mechanika Maszyn „”Mech-Masz” decydująca o celach i środkach przetwarzania danych osobowych
   b) **ABI-**Administrator Bezpieczeństwa Informacji
   c) **ASI-** Administrator Systemów Informatycznych
   d) **Ustawa-** ustawa o ochronie danych osobowych
   e) **Rozporządzenie-** Rozporządzenie Ministra Spraw wewnętrznych i Administracji z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
   f) **Przetwarzanie danych**- jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i

usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych

g) **Dane osobowe-** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
h) **Poufność danych-**właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,

Osoby odpowiedzialne za ochronę danych osobowych

1. Administrator Danych
   Mechanika Maszyn „Mech-Masz" Henryk Szczeciński
   88-400 Żnin ul. Szpitalna 20/ Jaroszewo 80
   REGON
2. Administrator Bezpieczeństwa Informacji : powołanie Administratora Bezpieczeństwa Informacji jest fakultatywne (załącznik nr 1 do Polityki Bezpieczeństwa)
   Administratorem Bezpieczeństwa Informacji może być osoba, która
   a) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych
   b) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych
   c) nie była karana za umyślne przestępstwo

   Do jego ustawowych obowiązków należy:

   a) zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez;
      - sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych
      - nadzorowanie , opracowywanie i uaktualnianie dokumentacji
      - zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych
      - prowadzenie rejestru zbiorów danych przetwarzanych przez Administratora Danych
      -prowadzi stały nadzór nad treścią Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym

- aktualizacja i modyfikacja w/w dokumentów
- nadawanie poszczególnym pracownikom upoważnień do przetwarzana danych osobowych oraz przeprowadzania dla nich szkoleń (wzór upoważnienia zał. nr 2 do Polityki Bezpieczeństwa)
- prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,
- monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych

3. Administrator Systemów Informatycznych
   Wyznaczenie Administratora Systemów Informatycznych jest fakultatywne wzór wyznaczenia załącznik nr. 3 do Polityki Bezpieczeństwa).
   Do uprawnień i obowiązków Administratora Systemów Informatycznych należą
   - nadawanie/nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych
   - nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów
   - podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie informatycznym
   -identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych
   - sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji zarządzania systemem informatycznym
4. Osoby upoważnione do przetwarzania danych osobowych
   a) Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym

b) Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
c) Procedura nadawanie upoważnień do przetwarzania danych osobowych stanowi załącznik nr 4 do Polityki Bezpieczeństwa

5.Umowy powierzenia przetwarzania danych osobowych

V Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych.

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
2. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
3. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „ czystego biurka”. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny postęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
4. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści (np. użycie niszczarki).
5. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

6. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
7. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

VI INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa Informacji i/ lub Administratorowi Systemów Informatycznych (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji / lub Administratora Systemów Informatycznych lub upoważnionej przez nich osoby, osoba powiadamiająca powinna:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe
   b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   c) udokumentować wstępnie zaistniałe naruszeni,

d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

3. Po przybyciu na miejsce naruszenia ochrony danych osobowych , Administrator Bezpieczeństwa Informacji lub Administrator Systemów Informatycznych lub osoba ich zastępująca :
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
   b) wysłuchuje relacji osoby zgłaszającej naruszenie, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem
4. Administrator Bezpieczeństwa Informacji i / lub Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.
5. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji i / lub Administrator Systemów Informatycznych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

VII KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Mechanice Maszyn „Mech-Masz” Henryk Szczeciński sprawuje Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych- w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
2. Administrator Bezpieczeństwa Informacji dokonuje czynności kontrolnych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
3. Administrator Bezpieczeństwa Informacji przeprowadza sprawdzenia w trybie:
   a) sprawdzenia planowego (zgodnie z harmonogramem)
   b) sprawdzenia doraźnego- w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji przedsięwzięcia wiadomości o naruszeniu

ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia

c) ABI opracowuje plan sprawdzeń zgodności przetwarzanych danych osobowych z przepisami o ochronie danych osobowych
d) po zakończeniu sprawdzenia ABI przygotowuje dla Administratora Danych sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest 1 raz w roku kalendarzowym na Przegląd Systemu Zarządzania w postaci elektronicznej lub papierowej
e) ABI ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych
f) Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych stanowi zał. 10 do Polityki Bezpieczeństwa
g) Wzór protokołu z kontroli lub czynności sprawdzających stanowi zał 11 do Polityki Bezpieczeństwa

VIII Spis przetwarzanych danych osobowych w organizacji

Mechanika Maszyn Mech-Masz”

Czyje dane są przechowywane	zakres przetwarzanych danych	Cel przetwarzania danych	Forma przechowywania	Forma zabezpieczeń	Osoby upoważnione do dostępu
Dane osobowe pracowników zatrudnionych na umowę o pracę					
Dane osobowe klientów pracowników działu marketingu					
Dane osobowe Klientów pozyskane w trakcie					

sprzedaży okuć meblowych na allegro					

IX Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Środki sprzętowe infrastruktury informatycznej	**Zastosowano tak / nie**	**uwagi**
Dostęp do systemu operacyjnego, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła	**tak**	
Zastosowano system rejestracji dostępu do systemu/ zbioru danych osobowych		
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim jak np., wirusy,robaki,konie trojańskie,rootkity	**tak**	
Użyto system Firewall		

do ochrony dostępu do sieci komputerowej		

Środki organizacyjne

Środki organizacyjne	**Zastosowano tak / nie**	**uwagi**
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	tak	
Prowadzona jest ewidencja osób upoważnionych do przetwarzana danych osobowych	tak	
Powołano Administratora Bezpieczeństwa Informacji	tak	
Opracowano i wdrożono Politykę Bezpieczeństwa	tak	
Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	tak	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami	tak	Zapoznanie poprzez : szkolenia wewnętrzne i zewnętrzne, informacje umieszczone w

dotyczącymi ochrony danych osobowych		rozporządzeniach ,na serwerze i tablicy informacyjnej
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	tak	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	tak	
Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętym pomieszczeniu	tak	
Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojących gaśnic	tak	
Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów	tak	

Środki fizyczne

Środek ochrony fizycznej	**Zastosowano Tak / nie**	**uwagi**
Zbiór danych osobowych przechowywany jest w zabezpieczonym pomieszczeniu	tak	
Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są systemem kontroli dostępu	tak	
Dostęp do pomieszczeń, w których		Pomieszczenia firmowe

przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych	tak	zabezpiecza system 8 kamer zamontowanych na zewnątrz budynku w newralgicznych miejscach
Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym pomieszczeniu w szafie zamykanej na klucz	tak	

INSTRUKCJA ZARZ ADZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W FIRMIE MECHANIKA MASZYN „MECH-MASZ" HENRYK SZCZECIŃSKI

I

1. Niniejsza instrukcja została opracowana zgodnie z wymaganiami rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.
2. Zawarte w tym dokumencie informacje są udostępniane selektywnie tylko tym osobom, którym są one potrzebne dla wykonywania powierzonych im zadań.
3. Niniejsza instrukcja jest dokumentem wewnętrznym Administratora Danych.
4. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym zobowiązani SA do zapoznania się z jej treścią, a fakt zapoznania się potwierdzić własnoręcznym podpisem na wykazie (wykaz stanowi zał. nr 1 do niniejszej instrukcji)

II

Rozpoczęcie, zawieszenie i zakończenie pracy w systemie

5. Przed rozpoczęciem pracy w systemie informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. W przypadku ich wykrycia należy niezwłocznie powiadomić o tym fakcie Administratora systemu informatycznego
6. W celu rozpoczęcia pracy użytkownik wykonuje logowanie do systemu używając nadanego loginu i hasła . Nadany login i hasło jest zmieniany w cyklu rocznym. Pełen zestaw nadanych loginów i haseł znajduje się w zabezpieczonym miejscu u Administratora systemu informatycznego.
7. Podczas nieobecności przy stanowisku komputerowym należy wylogować się z systemu bądź uruchomić wygaszacz ekranu.
8. Po zakończeniu pracy w systemie należy wylogować się z systemu i wyłączyć stację roboczą.
9. Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia zał. nr 2 do niniejszej instrukcji).
10. Za rejestrowanie uprawnień do przetwarzania danych osobowych odpowiada Administrator bezpieczeństwa informacji.
11. Może wystąpić zawieszenie korzystania z systemu :
    a) Planowe zawieszenie prac (związane np. z konserwacją)jest poprzedzone informacją ASI dla wszystkich upoważnionych pracowników, przynajmniej 30 min przed planowanym zawieszeniem).
12. Stosowane zabezpieczenia:
    a) Dane osobowe przetwarzane i gromadzone w formie elektronicznej, gromadzone SA na dyskach zabezpieczonego serwera plików w serwerowni oraz stacji roboczej w sekretariacie.
    b) Kopia bezpieczeństwa wykonywana jest na dysku zewnętrznym umieszczonym w zabezpieczonej serwerowni i zabezpieczonym hasłem.
    c) Nieaktualne nośniki danych osobowych w formie papierowej lub elektronicznej zostają trwale niszczone (zasady niszczenia

dokumentów zawierające istotne dane osobowe w firmie Mech-Masz stanowią zał. nr 3 do niniejszej instrukcji)

d) System komputerowy stacji roboczej – serwer, zabezpieczony jest programem antywirusowym Kaspersky Antivir (podlegający systematycznej aktualizacji). Dodatkowo dane baz danych programów używanych w firmie zabezpieczone są za pomocą 24- bitowego chroniącego foldery.

Prawa do wykonywania backupów baz danych oraz jakiekolwiek ingerencje w strukturę baz danych posiada jedynie