POLITYKA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH MJS SP. Z O.O.

 NIP: 521 388 41 03 ul. Fryderyka Chopina 41 lok. 2 20-230 Lublin

I. Postanowienia ogólne

1. Polityka określa zasady i sposób ochrony informacji, dokumentów, materiałów i danych oraz infrastruktury informatycznej przed nieuprawnionym ujawnieniem lub dostępem bądź zniszczeniem, jako stanowiących tajemnicę w rozumieniu postanowień niniejszej polityki i podlegających ochronie, a także obejmuje regulację obowiązków zatrudnionych w zakresie:
- używania sprzętu i oprogramowania komputerowego,
- łączenia się z siecią Internet lub innymi sieciami bądź obcymi urządzeniami komputerowymi (informatycznymi) i pocztą elektroniczną,
- używania zewnętrznych nośników, dyskietek i dysków w sprzęcie Spółki oraz zabezpieczenia mienia w tym zakresie.

2. Definicje pojęć:
- „informacja" objęta tajemnicą jest każda informacja jeżeli jest niejawna lub objęta tajemnicą na podstawie ustaw szczególnych lub została zaklasyfikowana / uznana jako wymagająca ochrony przed nieuprawnionym ujawnieniem na mocy postanowień niniejszej polityki, w tym również dane osobowe osób fizycznych – pracowników, kontrahentów i konsumentów (informacje chronione);
- „dokument" - każda utrwalona informacja, stanowiąca tajemnicę, zwłaszcza na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji (nośnikach danych) w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również każda informacja utrwalona na elektronicznych nośnikach danych;
- „materiał" jest dokument w rozumieniu przedmiotowym oraz przedmiot lub dowolna jego część, w szczególności urządzenie lub wyposażenie, jeżeli zostały objęte ochroną jako stanowiące informacje będące tajemnicą (np. modele, prototypy, itp.);
- „zatrudniony - pracownik, zleceniobiorca, wykonawca lub usługodawca bądź osoby przez nich zatrudnione, świadczące pracę lub usługi w siedzibie i innych lokalach Przedsiębiorcy, spółkach zależnych lub powiązanych;
-„infrastruktura techniczna/system informatyczny" – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji stosowanych w firmie w celu przetwarzania i ochrony informacji/danych, spełniających wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania informacji/danych",

-„nośniki informacji / danych” - materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej (płyta Cd, odtwarzacz płyt Cd, pamięć USB, interfejs USB w komputerze, karta micro SD, urządzenia elektroniczne z wbudowaną pamięcią;
-„zabezpieczenie systemu informatycznego” – wdrożenie właściwych środków administracyjnych, technicznych oraz ochrony przez modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem informacji/danych, a także ich utratą”;
-„firma”- MJS Sp. z o.o. z siedzibą w Lublin ul. Fryderyka Chopina 41 lok. 2.
3. Zasadą jest jawność informacji i prawa jej udostępniania, chyba że w trybie tej polityki lub na podstawie ustawy informacja jest niejawna lub objęta tajemnicą z innego tytułu.
4. Firma zapewnia i realizuje bezpieczeństwo informacji w systemach IT poprzez zapewnienie:
− poufności informacji/danych – pod którą rozumie się uniemożliwienie dostępu do danych osobom trzecim,
− integralności informacji/danych – pod którą rozumie się zapewnienie dokładności i kompletności informacji/danych i metod ich przetwarzania oraz uniknięcie nieautoryzowanych zmian danych,
− dostępności informacji/danych – pod którą rozumie się zapewnienie dostępu do informacji/danych osobom uprawnionym zawsze wtedy, gdy jest wymagane,
− rozliczalności działań – pod którą rozumie się zapewnienie, że jakiekolwiek działania na danych (przetwarzanie) jest rejestrowane w systemie informatycznym wraz z możliwością identyfikacji tego, kto uzyskał dostęp i/lub dokonał działania.
Firma stosuje adekwatne do sytuacji środki aby zapewnić bezpieczeństwo informacji w Firmie.

II. Przedmiot ochrony.

Na warunkach polityki ochroną obejmuje się następujące zakresy i przedmiot:

1. Chronione w ramach obowiązków publiczno-prawnych.

1.1. Sfera prywatności i dobra osobiste (art. 47 Konstytucji, art. 23 Kodeksu cywilnego)

Obowiązek ochrony informacji obejmuje:
- ochronę prawną życia prywatnego, w tym również rodzinnego, czci i dobrego imienia oraz informacje o majątku.

1.2. Dane osobowe osoby fizycznej (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2015 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, w sprawie swobodnego przepływu takich danych)

Obowiązek ochrony obejmuje:
1) każdą informację, na podstawie której można określić tożsamość danej osoby powiązaną z danymi chronionymi;
2) każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie czyli zbiór danych,
3) przetwarzanie danych w rozumieniu zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania danych, jak również każdej innej operacji przetwarzania wykonywanej w systemach informatycznych, jest możliwe tylko w trybie przewidzianym ustawą o tyle, o ile nie naruszają dobra publicznego, dobra osoby, której dotyczą lub dóbr osób trzecich.

1.3. Tajemnice według Prawa pracy

Obowiązek ochrony obejmuje dokumentację w sprawach związanych ze stosunkiem pracy:
1) dokumenty urzędowe lub osób prywatnych (rekomendacje, opinie) albo wytworzone przez firmę, dokumenty zgromadzone w związku z ubieganiem się o zatrudnienie,
2) dokumenty dotyczące nawiązania stosunku pracy oraz przebiegu zatrudnienia pracownika (karta ewidencyjna czasu pracy, imienna karta/lista wypłacanego wynagrodzenia za pracę i innych świadczeń związanych z pracą),
3) dokumenty związane z ustaniem zatrudnienia,
4) dokumenty dotyczące karania pracownika i wykroczeń dyscyplinarnych.

5) Oceny pracy, opinie i inne dokumenty, których ujawnienie może naruszyć dobra osobiste pracownika, w tym dane o wynagrodzeniu za pracę, podatkach, w tym PIT-y.

1.4. Tajemnica skarbowa (Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa)

Obowiązek ochrony obejmuje w szczególności:

1) dane mieszczące się w składanych przez podatników, płatników i inkasentów deklaracjach i innych dokumentach oraz wszelkie informacje podatkowe przepisane prawem

2) akta spraw prowadzonych przez organy podatkowe i organy kontroli skarbowej

3) informacje przekazane organom podatkowym przez Spółkę o zdarzeniach wynikających ze stosunków cywilno-prawnych albo Prawa pracy w zakresie wymaganym przepisami prawa.

1.5. Tajemnica bankowa (Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe)

Obowiązek ochrony obejmuje:

1) wszystkie wiadomości dotyczące czynności bankowych i osób będących stroną umowy, uzyskane w czasie negocjacji oraz związane z zawarciem umowy z bankiem i jej realizacją, z wyjątkiem wiadomości, bez ujawnienia których nie jest możliwe należyte wykonanie zawartej przez bank umowy;

2) wszystkie wiadomości dotyczące osób, które nie będąc stroną umowy, o której mowa w pkt. 1, dokonały czynności pozostających w związku z zawarciem takiej umowy, z wyjątkiem przypadków, gdy ustawa przewiduje ujawnienie takich czynności (art. 104 ust. 1 ustawy Prawo bankowe).

2. Dane chronione w ramach obowiązków prywatno-prawnych.

III. Tajemnica przedsiębiorstwa

Obowiązek ochrony obejmuje nie ujawniane do wiadomości publicznej (niepublikowane) informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa, które u przedsiębiorcy w trybie niniejszej polityki uznano za chronione i objęto tajemnicą przedsiębiorcy.

2.1.1. Rodzaje informacji objętych tajemnicą przedsiębiorstwa:

2.1.2. Informacje techniczne i technologiczne (przemysłowe)

- metodyki i technologie,
- dokumentacje,
- projekty programów szkoleniowych, znaków towarowych, nazw produktów, projektów graficznych do czasu skierowania do rejestracji praw ochronnych lub patentowych,

2.1.3. Informacje handlowe (tajemnica handlowa)

W zakresie zamówień:

- ilości zamówionych przez oznaczonych klientów usług,
- liczba i adresy oraz dane osobowe klientów,
- zbiory danych dostawców i odbiorców oraz dotyczące reklamacji,

2.2. Tajemnice firmy:

1) Decyzje Przedsiębiorcy w przedmiocie :

- określenia znaków towarowych – logo, nazwy własnej firmy, jego zmiany do czasu rejestracji, udzielenie licencji i pozwolenia na używanie przez osoby trzecie w ramach umów franchisingowych lub innych do czasu realizacji,
- wynagrodzeń

2) Decyzje Przedsiębiorcy dotyczące:

- zaciągania kredytów,
- zbywania i nabywania majątku trwałego.
- zasad utworzenia i wykorzystania funduszów celowych i darowizn oraz sponsoringu,

3)Dane dostępowe do systemów IT.

IV. Zakres podmiotowy zobowiązanych do ochrony

1. Osobami zobowiązanymi do ochrony, organizacji i nadzoru nad zabezpieczeniem informacji chronionych i bezpieczeństwem informatycznym w rozumieniu niniejszej polityki są właściciel oraz wszyscy pracownicy i współpracownicy firmy.
2. Osoby zobowiązane mają obowiązek zapewnienia ochrony informacji chronionych, w tym dokumentów, materiałów i danych na zasadach i w oparciu o niniejszą politykę.
3. Zatrudnionymi zobowiązanymi do stosowania się do obowiązków wynikających z Regulaminu są osoby fizyczne zatrudnione także na podstawie Umów: agencyjnej, o dzieło, pośrednictwa, akwizycji lub innej umowy mieszanej i nienazwanej z której wynika obowiązek wykonywania dla firmy lub w jej imieniu czynności prawnych lub faktycznych lub prawo przebywania na terenie obiektów firmy lub dostęp do sieci teleinformatycznej firmy.
4. Kontrahentem zobowiązanym do stosowania się do obowiązków wynikających z polityki są podmioty gospodarcze lub inne osoby prawne lub jednostki organizacyjne (spółki osobowe), które przyjmują do wykonywania prace na terenie przedsiębiorstwa (zakładów, oddziałów) Spółki lub uzyskują dostęp do ksiąg lub dokumentów Spółki bądź do sieci teleinformatycznej Spółki.

V. Dostęp do informacji chronionej, bezpieczeństwo informatyczne.

1. Każdy pracownik lub osoba zatrudniona na podstawie innego stosunku umownego przez przystąpieniem do wykonywania obowiązku podpisuje Oświadczenie o zapoznaniu się z zasadami polityki. Zarząd zapewnia okresowe szkolenia pracowników w zakresie bezpieczeństwa informatycznego.
2. Decyzje o zakresie dostępu do informacji chronionej podejmuje Zarząd.
3. Zatrudnieni w firmie mogą posługiwać się wyłącznie sprzętem i oprogramowaniem zakupionym przez Przedsiębiorcę, chyba że właściciel udzieli indywidualnej zgody na korzystanie z konkretnego obcego sprzętu lub oprogramowania, w innych sprawach w określonym przypadku i czasie. Każdy zatrudniony zobowiązany jest do ochrony swoich danych dostępowych do systemu informatycznego przedsiębiorstwa, w tym hasła dostępu poprzez jego nieprzekazywanie nieuprawnionym osobom trzecim, ochronę przed nieuprawnionym dostępem czy kradzieżą przez osoby trzecie.4. Stacje robocze podlegają zabezpieczeniu przed nieautoryzowanym dostępem osób trzecich. Własny sprzęt komputerowy (informatyczny), oprogramowania, dyski i dyskietki oraz inne urządzenia peryferyjne Zatrudnionego lub osób trzecich mogą być wnoszone na teren firmy lub łączone bądź wykorzystywane do/w sprzęcie firmy wyłącznie za zgodą właściciela odrębnie dla każdego przypadku jednorazowo. Ten sam tryb obowiązuje w przypadku przenoszenia niezabezpieczonych danych poza teren firmy na nośnikach elektronicznych (pendrive, nośniki CD, etc.).5. Łączenie się z siedziby firmy przy użyciu sprzętu, łączy, sieci z siecią Internet, pocztą elektroniczną, innymi sieciami lub użytkownikami jest dozwolone wyłącznie w zakresie, w miejscach i przy użyciu sprzętu firmy na który jest stała autoryzacja lub wydał na to zgodę właściciel. Korzystanie z systemu informatycznego firmy w celach prywatnych jest niedozwolone.6. Każdorazowe zalogowanie się, wejście do sieci wewnętrznej Spółki, wyjście z niej na zewnątrz, instalowanie programów, wprowadzanie danych z dysków lub dyskietek musi być poprzedzone sprawdzeniem i zapewnieniem, że jest zainstalowany i działa odpowiedni program antywirusowy zabezpieczający urządzenia firmy oraz dane przed utratą lub uszkodzeniem. Każdy przypadek wykrycia lub podejrzenia obecności„wirusa” należy zgłaszać właścicielowi.7. W przedsiębiorstwie stosuje się następujące kategorie środków zabezpieczeń danych:- zabezpieczenia fizyczne, w tym sposób i miejsce przechowywania elektronicznych nośników informacji/danych, kopii zapasowych,- zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej,- zabezpieczenia informatyczne.
8. W ramach zabezpieczenia danych ochronie w firmie podlegają: MJS Sp. z o.o. Ul. Fryderyka Chopina 41 lok. 2 20-230 Lublin Tel. +(48) 666 889 834 mail: kontakt@asteon.pl

- infrastruktura informatyczna, w tym sprzęt komputerowy, serwery, komputery osobiste (laptopy), drukarki i inne urządzenia zewnętrzne,
- oprogramowanie, w tym kody źródłowe, programy, systemy operacyjne, narzędzia programowe,
- dane zapisane na dyskach i dane podlegające przetwarzaniu w systemie informatycznym,
- hasła użytkowników, które powinny być okresowo zmieniane i przechowywane w formie zaszyfrowanej,
- użytkownicy i administratorzy obsługujący i używający system,
- dokumentacja – zawierająca dane systemu, techniczna,
- wydruki,
- związana z przetwarzaniem danych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego albo funkcjonują niezależnie od niego.

9. Podstawowymi stosowanymi środkami zabezpieczania danych w systemie informatycznym przedsiębiorstwa są:
- hasła dostępu do systemu,
- hasła dostępu do aplikacji,
- wygaszacze ekranu,
- stopniowanie uprawnień,
- stosowanie narzędzi ochrony antywirusowej, w tym oprogramowania antywirusowego, systemu typu firewall, odpowiedniej konfiguracji i aktualizacji używanych programów,
- okresowe archiwizowanie danych na wypadek awarii (kopie zapasowe)

VI. Kontrola i nadzór

1. Jakiekolwiek podejrzenie naruszenia bezpieczeństwa informatycznego w firmie podlega niezwłocznemu zgłoszeniu (powiadomieniu) ustnie lub za pośrednictwem poczty elektronicznej do Prezesa Zarządu.2. Właściciel okresowo wykonuje wewnętrzny lub zewnętrzny audyt bezpieczeństwa mający na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.3. Odpowiedzialność i kary: naruszenie obowiązków wynikających z niniejszej polityki oraz umowy zawartej z pracownikiem, stanowi rażące naruszenie obowiązków pracowniczych i będzie upoważniać Przedsiębiorcę do dochodzenia naprawienia szkody majątkowej albo zapłaty kary pieniężnej.

VII. Wprowadzenie polityki ochrony danych osobowych.

Politykę ochrony danych osobowych wprowadza się z dniem 06.01.2022. Za wykonanie obowiązków związanych z zastosowaniem polityki i nadzór w tym zakresie odpowiada Prezes Zarządu.