POLITYKA BEZPIECZEŃSTWA
WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
W ART 'N' MEDIA FUJARSKA S.K.A.
Z SIEDZIBĄ W WOJKOWICACH

Spis treści:

Polityka bezpieczeństwa:

Instrukcja dotycząca sposobu zarządzania systemem informatycznym:

I. Postanowienia ogólne.

§ 1

1. Celem niniejszej Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych:

   - przetwarzanych za zgodą Użytkowników w celu korzystania przez Użytkowników z Portalu dostępnego pod adresem www.twoja.tv oraz świadczenia na ich rzecz Usług w ramach portalu dostępnego pod adresem www.twoja.tv ;

   przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, w tym zapewnienie zachowania ich poufności, integralności i rozliczalności.
2. Polityka Bezpieczeństwa obowiązuje wszystkich pracowników ART'N'MEDIA Fujarska S.K.A., bez względu na zajmowane stanowisko, czy charakter pracy oraz wszystkie podmioty współpracujące na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.
3. Przetwarzanie danych osobowych w ART'N'MEDIA Fujarska S.K.A. odbywa się zarówno formie tradycyjnej (akta osobowe), jak i za pomocą systemów informatycznych (pozostałe). Dane osobowe przechowywane są na serwerze własnym ART'N'MEDIA Fujarska S.K.A. oraz zewnętrznym, zgodnie z zasadami ustalonymi w umowie zawartej z Quicktel Sp. z o.o., gwarantującej zachowanie wymaganych prawem zasad ochrony danych osobowych.
4. Funkcję Administratora Bezpieczeństwa Informacji pełno osoba wskazana w załączniku nr 6.

5. Funkcję Administratora Systemu Informatycznego pełni osoba wskazana w załączniku nr 7, co nie wyklucza korzystania przez ART'N'MEDIA Fujarska S.K.A. z pomocy zewnętrznej firmy informatycznej, przy zachowaniu zasad wynikających z przedmiotowej Polityki Bezpieczeństwa.

§ 2.

Pojęcia użyte w przedmiotowym dokumencie mają następujące znaczenie:

1) **ABI**- **Administrator Bezpieczeństwa Informacji**, przez którego należy rozumieć osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony, określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów prawa;
2) **Usługodawca lub Administrator danych osobowych lub Administrator**- należy przez to rozumieć ART'N'MEDIA Fujarska S.K.A., z siedzibą w Wojkowicach przy ulicy Sobieskiego 509, wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego w Sądzie Rejonowym Katowice-Wschód w Katowicach, VIII Wydział Gospodarczy KRS pod numerem: 0000410633, REGON: 242853028, NIP: 6252445928, reprezentowany przez *Komplementariusza bądź inną osobę, której udzielono pełnomocnictwa do reprezentowania Spółki;*
3) **ASI- Administrator Systemu Informatycznego**- osoba odpowiedzialna za funkcjonowanie systemu informatycznego, w tym jego sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych;
4) **Dane osobowe** - wszelkie informacje umożliwiające zidentyfikowanie osób fizycznych korzystających z Usług lub zatrudnionych w Spółce;
5) **Identyfikator**- należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracowników w systemie informatycznym tzw. login;
6) **Pracownik** - należy przez to rozumieć osobę zatrudnioną w formie umowy o pracę lub umowy cywilno-prawnej;
7) **Klient** – osoba fizyczna nieprowadząca działalności gospodarczej, przedsiębiorca, a w tym także osoba fizyczna prowadząca działalność gospodarczą bądź osoba prawna, uprawniony do zawarcia z Usługodawcą Umowy;
8) **Organizacja** – Klient który nie jest przedsiębiorcą a jest instytucją samorządową bądź organem samorządu terytorialnego, w tym także ich jednostką organizacyjną, któremu Usługodawca oferuje świadczenie Usług,
9) **Partner** – podmiot współpracujący z Usługodawcą przy świadczeniu Usług.
10) **Dane Identyfikacyjne** – dane obejmujące oznaczenie i dane Klienta, Organizacji, Usługobiorcy a w tym siedziba, miejsce wykonywania działalności, NIP, REGON, KRS, CEIDG,
11) **Usługi** – usługi świadczone przez Usługodawcę przy pomocy Portalu, z pomocą lub bez pomocy Partnera,
12) **Portal** – oprogramowanie oraz treści elektroniczne wytworzone bądź zestawione i skonfigurowane przez Administratora, dostępne w publicznej sieci Internet pod adresem www.twoja.tv lub domenami podrzędnymi, w tym także obejmujące Profil Użytkownika i Konto Użytkownika,
13) **Konto Użytkownika** – konto Użytkownika utworzone w procesie Rejestracji w Portalu, utrzymywane i prowadzone dla Użytkownika przez Administratora pod unikalną nazwą, obejmujące między innymi dane Użytkownika oraz informacje o działaniach Użytkownika w ramach Portalu dostępne po dokonaniu autoryzacji w sposób ustalony przez Administratora, zabezpieczone loginem i hasłem dostępu ustalonymi przez Użytkownika,
14) **Profil Użytkownika** – miejsce w Portalu, w którym Użytkownik po zalogowaniu do Konta Użytkownika może obsługiwać Konto Użytkownika, edytować i zmieniać dane Użytkownika,
15) **Koordynator Użytkownika** – osoba upoważniona przez Klienta, Organizacje bądź Usługobiorcę do zarządzania Profilem Użytkownika,
16) **Opiekuna Użytkownika** – specjalista koordynujący współpracę Usługodawcy z Użytkownikiem bądź Usługobiorcą, wyznaczany przez Usługodawcę spośród swoich pracowników bądź spośród Partnerów,
17) **Sieć Telekomunikacyjna** – urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną,

18) **System Teleinformatyczny** - zespół współpracujących lub połączonych ze sobą urządzeń telekomunikacyjnych, informatycznych (w tym komputerów) i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez Sieci Telekomunikacyjne,
19) **Plik Cookie** – dane tekstowe wysyłane przez System Teleinformatyczny Usługodawcy i zapisywane po stronie Użytkownika, Klienta, Organizacji bądź Usługobiorcy - odczytywane przez Portal podczas korzystania z Usług.
20) **Umowa** – umowa o świadczenie usług drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2013 r., poz. 1422 z późn. zm.).
21) **Użytkownik** – Klient bądź Organizacja.
22) **Ustawa** - należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
23) **Przetwarzanie danych** - rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
24) **Poufność danych** - jest to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
25) **Integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione, lub zniszczone w sposób nieautoryzowany.
26) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

II. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

W ART'N'MEDIA Fujarska S.K.A. dane osobowe przetwarzane są w następujących zbiorach:

1) W formie elektronicznej jako
   a) **Rejestr Klientów**
   b) **Konta Użytkowników**

Dane osobowe w formie elektronicznej przetwarzane są za pomocą programu o nazwie MySQL.

III. Zakres danych osobowych przetwarzanych w placówce.

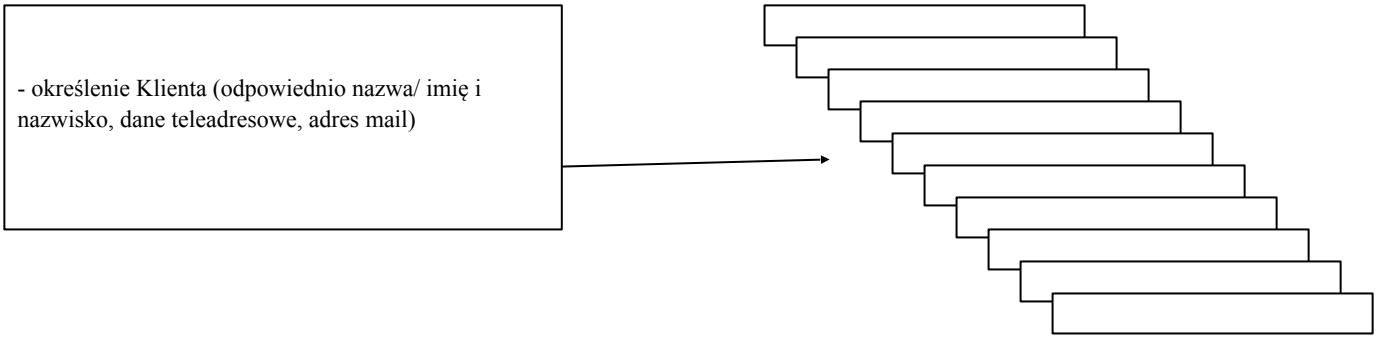
W utworzonych i wydzielonych zbiorach danych osobowych przetwarzane są następujące dane:

W Rejestrze Klientów przetwarzane są następujące dane:
- określenie Klientów (odpowiednio nazwa/ imię i nazwisko, dane teleadresowe, adres mail)

W ramach Konta Użytkownika przetwarzane są następujące dane:
- Dane Identyfikacyjne
- nazwisko i imiona przedstawicieli Klienta, Organizacji i Usługobiorcy, osób przez niego upoważnionych lub innych wskazanych jako kontaktowe w wykonywaniu Usług i Umowy,
- adres do korespondencji, jeżeli jest inny niż adres siedziby
- adresy elektroniczne
- informacje o działaniach Klienta bądź Organizacji w ramach Portalu, o Usługach i rozliczeniach Usług

<u>Przepływ informacji miedzy rejestrami a kontami klientów</u>

REJESTR Konta Klientów



IV.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe.

Przetwarzanie danych osobowych odbywa się w pomieszczeniach w siedzibie ART'N'MEDIA Fujarska S.K.A. oraz na serwerach zlokalizowanych w Data Center 4DC w Katowicach przy ul. Adamskiego 8.

- pomieszczenia zajmowane przez Pracowników gdzie przetwarzane są informacje i dane osobowe (w tym wpisywane, modyfikowane, kopiowane)

Dane w formie elektronicznej przechowywane są na serwerach zlokalizowanych w Data Center 4DC w Katowicach przy ul. Adamskiego 8.

Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Zabrania się przebywania osób postronnych w pomieszczeniach Spółki, w których przetwarzane są dane osobowe bez obecności osób upoważnionych.

V. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych

1. Każdy Pracownik przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:
   - ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
   - rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
   - niniejszą polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym
2. Zapoznanie się z powyższymi dokumentami Pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik nr 1.
3. Przetwarzania danych osobowych może dokonywać jedynie Pracownik upoważniony przez administratora danych osobowych. Wzór upoważnienia stanowi Załącznik nr 2.
4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu przez ABI dla każdego Pracownika unikalnego identyfikatora ze wskazaniem zakresu dostępnych danych i operacji.
5. Hasło pierwszego logowania w systemie ustanawia ABI. Każdy Pracownik ma obowiązek dokonać jego zmiany na indywidualne, co najmniej ośmioznakowe hasło, w skład którego muszą wchodzić małe i duże litery, cyfry lub znak specjalny. Hasło winno być zmieniane co 30 dni.

VI. Odpowiedzialność

1. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
2. Pracownik ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu z wyjątkiem sytuacji, kiedy ABI użyje hasła Pracownika podczas jego

nieobecności. ABI ma obowiązek sporządzić z tego zdarzenia protokół, z którym zostaje zapoznany Zarząd oraz Pracownik, którego hasło zostało użyte. Po zapoznaniu się z protokołem, użytkownik systemu ma obowiązek dokonać natychmiastowej zmiany hasła dostępu i przekazać je ABI.

3. Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
4. ABI może odebrać uprawnienia pracownikowi z podaniem daty oraz przyczyny odebrania uprawnień. W uzasadnionej sytuacji ABI może odebrać uprawnienia w sposób natychmiastowy. Z takiego postępowania ma on sporządzić notatkę służbową do wiadomości Zarządu i Pracownika, którego sprawa dotyczy.
5. Uprawnienia Pracownika, który je utracił, należy niezwłocznie wyrejestrować z systemu informatycznego. Identyfikator Pracownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym.

VII. **Rejestr**

1. ABI jest zobowiązany do prowadzenia i ochrony rejestru Pracowników *i ich uprawnień w systemie informatycznym*
2. Rejestr musi odzwierciedlać aktualny stan systemu w zakresie Pracowników i ich uprawnień *oraz umożliwić przeglądanie historii zmian w systemie informatycznym*.
3. Rejestr, którego wzór stanowi Załącznik nr 3 zawiera:

- imię i nazwisko,
- identyfikator Pracownika,
- zakres uprawnienia,
- datę nadania uprawnień,
- datę odebrania uprawnień,
- przyczynę odebrania uprawnień,
- podpis ABI.

VIII. Zasady udostępniania danych osobowych

1. Dopuszcza się przekazywanie danych osobowych, o których mowa powyżej Parterom w celu wykonanie Usług oraz podmiotom i organom upoważnionym na podstawie odrębnych przepisów.
2. Z czynności przekazania danych, o których sporządza się protokół przekazania.
3. ABI zobowiązany jest do prowadzenia ewidencji udostępniania danych osobowych ze zbiorów.

IX. Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

1. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą Administratora danych osobowych i za wiedzą Administratora Bezpieczeństwa Informacji.
2. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.
3. ABI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:

- dokonano konfiguracji oprogramowania na komputerach przenośnych poprzez, szyfrowanie dysku, wprowadzenie hasła na twardy dysk, wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe, jak również ustawienie żądania przez system hasła po krótkim okresie

bezczynności (pojawianie się wygaszacza ekranu) - zabezpieczono dane osobowe poprzez szyfrowanie dysku
- dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym,
- przeprowadzono aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.
- dokonanie instalacji i konfiguracji tzw. zapory ogniowej sprzętowej lub programowej

4. Administrator bezpieczeństwa informacji jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych, w szczególności ewidencja obejmuje:

- typ i numer seryjny komputera przenośnego,
- imię i nazwisko osoby będącej użytkownikiem komputera,
- oprogramowanie chroniące dane osobowe zainstalowane na komputerze,
- rodzaj i zakres danych osobowych przetwarzanych na komputerze przenośnym.

5. W razie zgubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia Administratora Bezpieczeństwa Informacji lub osoby uprawnionej.
6. Użytkownik komputera przenośnego zobowiązany jest do:

- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności: transportowania komputera w bagażu podręcznym, nie pozostawiania komputera w samochodzie, przechowalni bagażu itp., zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych.
- korzystania z komputera w sposób minimalizujący ryzyko zaobserwowania przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego oraz z użyciem publicznych punktów dostępowych do sieci Internet (tzw. hot spotów),
- nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
- zabezpieczania dysku komputera przenośnego oraz dostępu do komputera przenośnego hasłem,
- blokowanie dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika poprzez uruchomienie wygaszacza ekranu i żądani ponownego wprowadzenia hasła,
- kopiowanie danych osobowych przetwarzanych na komputerze przenośnym na serwer zewnętrzny w celu umożliwienia wykonania kopii awaryjnej tych danych,
- umożliwienia, poprzez podłączenie komputera do sieci Internet, aktualizacji wzorców wirusów w programie antywirusowym,
- utrzymanie konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,
- wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
- zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

X. Procedura postępowania w sytuacji naruszenia Polityki bezpieczeństwa.

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym ASI, ABI lub inną upoważnioną osobę.
2. ASI po otrzymaniu powiadomienia:

- sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
- sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
- sprawdza jakość komunikacji w sieci telekomunikacyjnej,
- poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

3. W przypadku stwierdzenia naruszenia zabezpieczeń danych administrator:

- podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),

- w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
- zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
- niezwłocznie przywraca prawidłowy stan działania systemu,
- dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
- sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia, zgodnie ze wzorem stanowiącym załącznik nr 4.

4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) ASI przekazuje Zarządowi.
5. ASI podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

- jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
- jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągnięcie konsekwencji przewidzianych prawem,
- jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organy ścigania.

XI. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

Serwerownia zabezpieczona jest odpowiednią instalacją alarmową, zbiory danych przechowywane są w pomieszczeniu zamykanym na klucz i odpowiednio zabezpieczonym, w tym usługami firmy ochroniarskiej.

Dodatkowo
- wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych – także z godzinach pracy;
- nieaktualne lub błędne wydruki zawierające dane osobowe są niszczone w niszczarkach

Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych:
- identyfikacja Pracownika w systemie poprzez zastosowanie uwierzytelnienia
- przydzielenie indywidualnego identyfikatora każdemu Pracownikowi
- zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity
- zabezpieczenie hasłami kont na komputerach
- ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiając wgląd w dane osobom nieupoważnionym
- automatyczne wygaszanie ekranu
- wymuszenie zmiany hasła co 30 dni

- instalacja zapory ogniowej (firewalla)

Formy zabezpieczeń przez nieautoryzowanym dostępem do baz danych za pomocą sieci teleinformatycznej – logiczne oddzielenie sieci wewnętrznej od sieci zewnętrznej, uniemożliwiające uzyskanie połączenia z baza danych spoza systemu informatycznego, jak również uzyskanie dostępu z systemu do sieci Internet

Formy zabezpieczenia serwerów

1. W zakresie fizycznych środków ochrony danych:
    a) serwery przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej,
    b) serwery przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej,
    c) pomieszczenia, w którym znajdują się serwery wyposażone są w system alarmowy przeciwwłamaniowy,
    d) kopie zapasowe/archiwalne danych przechowywane są na oddzielnych serwerach,
    e) pomieszczenie, w którym znajdują się serwery zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

2.W zakresie infrastruktury informatycznej i telekomunikacyjnej:

    a) zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny serwerów przed skutkami awarii zasilania,
    b) dostęp do systemu operacyjnego komputera, który jest serwerem zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
    c) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł administratora,
    d) zastosowano macierz dyskową w celu ochrony danych znajdujących się na serwerach przed skutkami awarii pamięci dyskowej,
    e) zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,
    f) użyto system Firewall do ochrony dostępu do sieci komputerowej.

XII. Postanowienia końcowe

Wprowadzenie niniejszej Polityki Bezpieczeństwa zostało poprzedzone audytem komputerów Spółki i zainstalowanego na nich oprogramowania. Zabrania się pracownikom lub osobom współpracującym samodzielnego instalowania jakiegokolwiek innego oprogramowania na komputerach, bez uprzedniego powiadomienia ASI i uzyskania jego zgody, po uprzednim wykluczeniu przez ASI zagrożenia bezpieczeństwa danych przez takie oprogramowanie.

W zakresie nieuregulowanym niniejszą Polityką Bezpieczeństwa zastosowanie mają przepisy powszechnie obowiązującego prawa, w tym:

- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami);
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

Polityka Bezpieczeństwa będzie weryfikowana i dostosowywana w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji Polityki Bezpieczeństwa odbywają się nie rzadziej niż raz w roku.

Opis struktury zbiorów danych, wskazujący na zawartość poszczególnych pól informacyjnych i powiązania między nimi, jest udostępniany przez Administratora Systemu Informatycznego.

We wszystkich umowach zawieranych przez Spółkę, które mogą dotyczyć przetwarzania danych osobowych, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania odpowiednich zapisów Polityki Bezpieczeństwa.

Integralną część Polityki Bezpieczeństwa stanowią następujące Załączniki:

- Załącznik nr 1 – oświadczenie pracownika
- Załącznik nr 2 – upoważnienie imienne do przetwarzania danych osobowych
- Załącznik nr 3 - ewidencja osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym
- Załącznik nr 4 - raport z naruszenia bezpieczeństwa danych osobowych
- Załącznik nr 5 - Instrukcja dotycząca sposobu zarządzania systemem informatycznym
- Załącznik nr 6 - wyznaczenie ABI
- Załącznik nr 7- wyznaczenie ASI

Załącznik nr 1

O Ś W I A D C Z E NI E

Ja, …….. (imię i nazwisko), mniejszym potwierdzam, iż w dniu …… (data) zostałem zapoznany z przepisami odnoszącymi się do ochrony danych osobowych objętymi
- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- Polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym ART'N'MEDIA Fujarska S.K.A. i zobowiązuję się do ich przestrzegania.;

jak również zostałem przeszkolony z obsługi systemu antywirusowego.

……
(podpis)

Wykaz osób, które zostały zapoznane z Polityką ochrony danych osobowych oraz Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

Lp.	Imię i Nazwisko	Stanowisko	Data	Podpis

Załącznik nr 2

Upoważnienie imienne Nr …….
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam Panią / Pana:……(imię i nazwisko osoby upoważnionej)

zatrudnioną w ..... na stanowisku: ……..
do przetwarzania od dnia ……r. danych osobowych
w z a k r e s i e
…….....
.....
...

Nadaję identyfikator:

……
(podpis)

Załącznik nr 3

Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym

L.p.	Identyfikatoru	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień w systemie	Data i podpis ABI	Data odebrania uprawnień w systemie oraz data i podpis ABI
1.						
	Zmiany danych**					
2.						
	Zmiany danych**					
3.						
	Zmiany danych**					
4.						
	Zmiany danych**					
5.						
	Zmiany danych**					

*Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie,

**Jeżeli zmiany danych dotyczą tylko niektórych rubryk, np. miejsca pracy; pozostałe rubryki w wierszu powinny zostać przekreślone, tak, aby było jasne, jakich danych dotyczyła zmiana.

Załącznik nr 4

Raport z naruszenia bezpieczeństwa danych osobowych
1.Data:Godzina:
(dd.mm.rrrr) (gg:mm)

2.Osoba powiadamiająca o zaistniałym zdarzeniu:
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

3. Lokalizacja zdarzenia:
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

5. Przyczyny wystąpienia zdarzenia:

6. Podjęte działania:

7. Postępowanie wyjaśniające:

(data, podpis ABI lub ASI)

Załącznik nr 5

Instrukcja dotycząca sposobu zarządzania systemem informatycznym

A. Zasady zabezpieczania sprzętu informatycznego, danych i oprogramowania

1. Kontroli podlega dostęp do pomieszczeń, w których znajduje się sprzęt komputerowy, w celu zabezpieczenia sprzętu oraz danych osobowych i oprogramowania przed ich wykorzystaniem lub zniszczeniem przez osoby trzecie.
2. Kopie danych zawartych w systemie tworzy się *co najmniej raz w miesiącu*. Kopia tworzona jest przez odpowiednie oprogramowanie. Każda następna kopia zapisywana jest w miejsce poprzedniej.
3. System informatyczny zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (antywirus - program Microsoft Security Esentials.
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (UPS)

4. Dane przechowane w kopii zapasowej są szyfrowane
5. Pracowników obowiązuje bezwzględny zakaz wynoszenia płyt lub innych nośników z oprogramowaniem lub innymi danymi poza teren siedziby Spółki, chyba że zgodę na taką czynność wyraził piśmie ABI lub ASI.
6. Urządzenia, dyski lub inne nośniki informacji przeznaczone do:

- likwidacji- pozbawia się danych poprzez formatowanie oraz fizyczne uszkodzenie, uniemożliwiające ich odczytanie,
- przekazania- pozbawia się zapisu zawierającego dane osobowe,
- naprawy- pozbawia się zapisu danych osobowych lub naprawia pod nadzorem osoby do tego upoważnionej przez ABI lub ASI.

7. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w Polityce Bezpieczeństwa, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

B Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Komputer uruchamia się po wprowadzeniu do niego hasła.
2. Przy wejściu do systemu przetwarzającego dane osobowe wprowadza się identyfikator oraz hasło dostępu.
3. Opuszczając czasowo stanowisko pracy blokuje się dostęp do konta.
4. Zakończenie pracy związanej z przetwarzaniem danych odpowiadać winno wszystkim regułom bezpieczeństwa informacji zawartym w przedmiotowej Polityce bezpieczeństwa.

C. Zabezpieczenie systemu przed nieuprawnionym dostępem

1. Dopuszcza się możliwość przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe pod następującymi warunkami:
   - na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe,
   - każdy e-mail wpływający do jednostki musi być sprawdzony pod kątem występowania wirusów,
   - aktualizacje programów antywirusowych muszą być dokonywane nie rzadziej niż raz w tygodniu (automatycznie przez program),
   - zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć,
   - zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.
2. Dostęp do sieci bezprzewodowej dla pracowników jest chroniony protokołem WPA2.
3. Każdy Pracownik musi zostać przeszkolony z obsługi programu antywirusowego, co poświadcza stosownym oświadczeniem.

4. Pracownicy są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym.

D Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Procedury naprawy sprzętu komputerowego:

a) naprawy sprzętu komputerowego dokonywać może jedynie wyspecjalizowana firma informatyczna.

b) naprawa sprzętu komputerowego użytkowanego w systemie poza siedzibą ART'N'MEDIA Fujarska S.K.A. musi zostać poprzedzona usunięciem z twardego dysku wszelkich aplikacji przetwarzających i zawierających dane o charakterze osobowym. ASI odpowiedzialny jest za stworzenie kopii tej bazy. Po powrocie z serwisu sprzętu komputerowego, ASI ponownie instaluje bazę danych, a jej kopia zostaje zniszczona.

2. Procedura przeglądu systemu:

przeglądu systemu dokonuje firma informatyczna obsługująca Spółkę pod względem informatycznym, na mocy odrębnego zlecenia.

E Do przetwarzania danych osobowych w systemie informatycznym dopuszczone są wyłącznie osoby przeszkolone w zakresie zasad przetwarzania danych osobowych i obsługi systemu informatycznego oraz posiadające upoważnienie do przetwarzania danych osobowych.

Załącznik Nr 6

ART’N’MEDIA Fujarska S.K.A. wyznacza jako Administratora Bezpieczeństwa Informacji:

.....

Załącznik Nr 7

ART’N’MEDIA Fujarska S.K.A. wyznacza jako Administratora Systemów Informatycznych:

.....