POLITYKA BEZPIECZEŃSTWA
firmy „Dreamtec” Sp z o.o.

wersja 2.0 z dnia 01.01.2017 r.

§ 1

Zagadnienia wstępne

1. Niniejszy dokument został przygotowany z myślą o zapewnieniu standardów bezpieczeństwa informacji w spółce ze szczególnym uwzględnieniem zgodności z prawem.
2. Szczegółowy zakres obowiązków i procedur postępowania w przypadku zagrożenia bezpieczeństwa informacji określony zostanie poniżej.
3. Poprzez bezpieczeństwo należy rozumieć stan faktyczny uniemożliwiający wykorzystanie, przepływ, modyfikację lub zniszczenie informacji w spółce przez osoby postronne lub nieupoważnione.
4. Dokument Polityki Bezpieczeństwa opracowany jest w oparciu o wytyczne zawarte w następujących aktach prawnych:
    a. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883),
    b. 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 (Dz.U. 2004 nr 100 poz. 1024),
    c. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 nr 0 poz. 719),
    d. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015 nr 0 poz. 745)

§ 2

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

1. Dane osobowe przetwarzane są na serwerach znajdujących się w Centrum przetwarzania i przechowywania danych
    a. „Sprint Data Center S.A." ul. Jagiellończyka 26;10-062 Olsztyn, REGON: 001339396, KRS 0000372363
    b. W zakresie centrum kopii zapasowych: „3S Data Center S.A." ul. Gospodarcza 12; 40-432 Katowice, REGON:241656774, KRS: 0000364798 oraz jego podwykonawcy w zakresie infrastruktury telekomunikacyjnej 3S S.A. ul. Ligocka 103 BUD.8 40-568 Katowice, REGON:277704261, KRS:0000095232. Podpowierzenie może być dokonane w celu świadczenia Wykonawcy przez 3S Data Center S.A. usług wsparcia technicznego oraz usług hostingowych.
2. Pomieszczenia Centrum przetwarzania i przechowywania zabezpieczone są przed dostępem osób trzecich. Poziom zabezpieczeń przed fizycznym dostępem osób trzecich i fizyczne zabezpieczenie danych przed kradzieżą i utratą bezpieczeństwa określone są polityką bezpieczeństwa powyższych Centrów.
3. Nośniki informacji są przechowywane w zamkniętej szafie.

§ 3

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Dane osobowe przetwarzane są przy wykorzystaniu systemu platformy serwerowej Linux.
2. Zbiorem danych osobowych objęte są dane osobowe użytkowników systemów: Platformy e-Dziennika MobiReg.
3. Dane osobowe obejmujące system Platforma e-Dziennika MobiReg, przetwarzane są przy użyciu relacyjnego systemu baz danych MySQL.

§ 4

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. W zbiorze danych systemu MobiReg dane wrażliwe przetwarzane są w następującym zakresie:
    a. Dane Ucznia: imię, drugie imię, nazwisko, PESEL, data urodzenia, ulica, miasto, województwo, płeć, oceny ucznia, obecności ucznia, numer w dzienniku, numer ewidencyjny, rok w klasie, klasa, indywidualny tok nauczania, obwód szkolny, rodzaj niepełnosprawności, informacje o kształceniu specjalnym, dane rodziców, eduid.
    b. Rodzica: imię, nazwisko, email, numer telefonu, adres, opieka nad uczniem
    c. Nauczyciela: imię, nazwisko, telefon, email, przedmioty nauczania i klasy
    d. Użytkownik systemu: login, hasło, email.

§ 5

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Zgodnie z Ust. „O ochronie danych osobowych" Art. 36. 1. „Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem." w celu

zabezpieczenia zbioru danych osobowych systemów przed dostępem osób nieupoważnionych wprowadza się odpowiednie rozwiązania techniczne i organizacyjne.

a. Dla Centrum przetwarzania i przechowywania danych „Sprint Data Center S.A.":
   i. **Bezpieczeństwo na poziomie ogólnym**. (zabezpieczenia techniczne i organizacyjne zawarte w Polityce Bezpieczeństwa Sprint Data Center). Na podstawie dokumentu „Sprint S.A. – wykaz posiadanych certyfikatów, koncesji i uprawnień" stwierdza się iż sposób prowadzenia i zakres dokumentacji, o której mowa w art. 39a ustawy o ochronie danych oraz środki organizacyjne i techniczne zastosowane w celu zapewnienia ochrony przetwarzanych danych są zgodne z przepisami rozporządzenia 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.:

I. Bezpieczeństwo fizyczne obiektu

Obiekt Sprint Data Center podzielony jest na strefy. Każda strefa posiada określone uprawnienia dostępu. Dostęp do strefy II i III jest ograniczony tylko do osób upoważnionych/uprawnionych oraz jest kontrolowany i monitorowany. Dodatkowo wstęp do strefy II i III obywa się pod nadzorem uprawnionych pracowników Sprint. Strefy Sprint Data Center:

1. Obiekt SDC (będący wyłączną własnością Sprint) – otoczenie budynku
   a. fizycznie ogrodzony
   b. monitoring wizyjny (24h/7 dni w tygodniu) całej posesji, rejestracja i archiwizacja obrazu z kamer
   c. stały osobowy nadzór 24h, 7 dni w tygodniu
2. Obiekt SDC – strefa I (ogólnie dostępna – Recepcja)
   a. monitoring wizyjny osób wchodzących do budynku (24h/7 dni w tygodniu), rejestracja i archiwizacja obrazu z kamer
   b. rejestracja osób zewnętrznych /gości
   c. system alarmowy wykrywający próby włamania do obiektu
   d. system p.poż. ogólnego przeznaczenia
   e. stały osobowy nadzór 24h, 7 dni w tygodniu
3. Obiekt SDC – strefa II (dostęp ograniczony, bezpośrednie zarządzanie serwerami z SDC)
   a. monitoring wizyjny osób wchodzących do strefy II (24h/7 dni w tygodniu), rejestracja i archiwizacja obrazu z kamer
   b. dwustronna elektroniczna kontrola dostępu do strefy II
   c. rejestracja osób zewnętrznych /gości
   d. system alarmowy wykrywający próby włamania do obiektu
   e. system p.poż. ogólnego przeznaczenia
   f. stały osobowy nadzór 24h, 7 dni w tygodniu
4. Obiekt SDC – strefa III (dostęp ograniczony, pomieszczenie – serwerownia)
   a. brak okien, drzwi antywłamaniowe
   b. monitoring wizyjny osób wchodzących i poruszających się w strefie III (24h/7 dni w tygodniu), rejestracja i archiwizacja obrazu z kamer
   c. dwustronna elektroniczna kontrola dostępu do strefy III
   d. rejestracja osób zewnętrznych /gości
   e. system alarmowy wykrywający próby włamania do obiektu
   f. koincydencyjny system p.poż. (system punktowy + system liniowy wczesnej detekcji pożaru typu VESDA)
   g. system gaszenia (bezpieczny dla ludzi i sprzętu komputerowego) oparty o aerozol

II. Bezpieczeństwo energetyczne

1. Układ zasilania gwarantujący ciągłość zasilania. System automatycznie wykrywa zanik napięcia ze strony Zakładu Energetycznego. W przypadku zaniku System Załączenia Rezerwy dokonuje przełączenia na Wewnętrzne Źródło Zasilania (agregat prądotwórczy). Układ zapewnia autonomię zasilania przez minimum 24h. Czas pracy może być wydłużony poprzez uzupełnienie paliwa.
2. Elementy systemu zasilania energetycznego
3. Własna stacja SN/NN 15kV zasilana dwutorowo z ringu ZE
4. Agregat prądotwórczy 730kVA jako źródło zasilania awaryjnego
5. System zasilaczy UPS pracujących w trybie pracy równoległej, układ redundantny N+1
6. Zasilanie szafy rack z dwóch różnych obwodów

III. Bezpieczeństwo środowiskowe

1. Zapewnienie właściwych parametrów środowiskowych (temperatura i wilgotność powietrza w serwerowni). Temperatura powietrza – 23°C ± 2°C; wilgotność względna powietrza – 50% ± 10%
2. Systemu klimatyzacji precyzyjnej i wentylacji
3. Klimatyzacja pracująca w układzie redundantnym N+1
4. Kontrola temperatury i wilgotności w pomieszczeniu serwerowni
5. Agregaty chłodnicze pracujące w układzie redundantnym
6. Redundantne tory czynnika chłodniczego
7. Wentylacja pomieszczenia

IV. Bezpieczeństwo infrastruktury informatycznej

1. Zapewnienie wysokiego poziomu dostępności w transmisji danych informatycznych dla świadczonych usług. Brak pojedynczego punktu awarii dla transmisji wewnętrznej i zewnętrznej. Infrastruktura informatyczna zapewnia możliwość monitorowania ruchu sieciowego.

V. Łącza dostępowe SDC

1. 3 niezależne łącza światłowodowe, różne trasy kablowe, różne punkty wejścia do budynku
2. Dostęp do punktu wymiany ruchu (ponad 100 krajowych operatorów)
3. Zdublowane routery brzegowe

VI. Wewnętrzna sieć komputerowa SDC

1. Warstwa szkieletowa 10Gb/s oparta na światłowodach,
2. Wszystkie połączenia w warstwie szkieletowej są zdublowane
3. Wszystkie urządzenia przełączające w warstwie szkieletowej są zdublowane
4. Warstwa dystrybucyjna 1Gb/s oparta na światłowodach,
5. Wszystkie połączenia w warstwie szkieletowej są zdublowane
6. Wszystkie urządzenia przełączające w warstwie szkieletowej są zdublowane
7. Warstwa dostępowa (dotyczy pojedynczej szafy rack) oparta o okablowanie miedziane 1Gb/s

VII. Bezpieczeństwo sieciowe

1. Systemy bezpieczeństwa typu firewall – urządzenia zdublowane
2. System wykrywania potencjalnych zagrożenia IDS/IPS

ii. <u>Bezpieczeństwo na poziomie jednostki serwerowej</u>

I. Zabezpieczenia warstwy fizycznej.

1. Stopień zabezpieczeń wg rozp. MSWiA z dnia 29 kwietnia 2004 r.: wysoki
2. Zarządzanie warstwą sprzętową (serwery, obudowa, przełączniki serwera DELL m1000, macierz VESSRaid) zabezpieczone odbywa przy użyciu szyfrowanego protokołu zabezpieczonego certyfikatem SSL.
3. Warstwa sprzętowa (przełączniki łączące serwery z internetem) wyposażona jest w firewall zabezpieczający przed atakami typu DDoS.
4. Konta do zarządzania zabezpieczone hasłem spełniającym wymogi wysokiego stopnia zabezpieczeń.

II. Zabezpieczenia warstwy programowej (środowiskowej).

1. Na serwerach zainstalowane jest środowisko wirtualizacyjne oparte na systemie operacyjnym Linux i hypervisorze KVM.
2. Środowisko wirtualizacyjne zabezpieczone jest przy pomocy programowego firewall-a chroniącego samo środowisko jak i serwery wirtualne.
3. Zarządzanie środowiskiem odbywa się przy użyciu szyfrowanego protokołu zabezpieczonego certyfikatem SSL.
4. Konta do zarządzania zabezpieczone hasłem spełniającym wymogi wysokiego stopnia zabezpieczeń.
5. Stosowane są odpowiednie polityki systemowe wymuszające zgodność haseł z poziomem zabezpieczeń: ”wysoki”.
6. System rejestruje czas i login-y dostępu do systemu, rejestrowane są zarówno połączenia udane jak i nieudane.

III. Zabezpieczenia warstwy programowej (systemowej).

1. W środowisku wirtualizacyjnym osadzone są serwery wirtualne zrealizowane na bazie dystrybucji DEBIAN systemu operacyjnego LINUX stanowiące podstawę systemową oprogramowania MobiReg – dziennik internetowy.
2. Zarządzanie serwerami odbywa się przy użyciu szyfrowanego protokołu zabezpieczonego certyfikatem SSL.
3. Konta do zarządzania zabezpieczone hasłem spełniającym wymogi wysokiego stopnia zabezpieczeń.
4. Stosowane są odpowiednie polityki systemowe wymuszające zgodność haseł z poziomem zabezpieczeń: ”wysoki”
5. System rejestruje czas i login-y dostępu do systemu, rejestrowane są zarówno połączenia udane jak i nieudane.

IV. Zabezpieczenia warstwy programowej (aplikacji).

1. Zbiór danych osobowych chroniony jest nowoczesnymi mechanizmami szyfrowania.
2. W celu zabezpieczenia systemu i ochrony danych osobowych wprowadza się zabezpieczenie firewall – system izolacji i selekcji połączeń z siecią zewnętrzną.
3. Dla zabezpieczenia zbioru danych osobowych wprowadza się system uwierzytelniania użytkowników zabezpieczony co najmniej 8-znakowym hasłem, zgodnie z postanowieniami ustawy i aktów wykonawczych.
4. Mechanizm zabezpieczania i uwierzytelniania użytkowników oraz procedury postępowania zostały szczegółowo opisane w dokumencie – ***„Instrukcja Zarządzania Systemem Informatycznym w Dreamtec sp. z o.o.”.***

V. Zabezpieczenia przed utratą danych (back-up)

1. Wykonywane są automatyczne kopie bezpieczeństwa (backup) serwera wirtualnego zawierającego system „Platfroma e-Dziennika MobiReg".
2. Wykonywane są niezależne kopie bezpieczeństwa baz danych programu „Platfroma e-Dziennika MobiReg". W/w kopie wykonywane są w trybie:
    a. kopie pełne: raz na miesiąc, okres przechowywania kopii 5 lat
    b. kopie pełne: raz na tydzień, okres przechowywania kopii 1 rok
    c. kopia pełne: raz na dzień, okres przechowywania kopii 2 miesiące
    d. kopia różnicowa: co dwie godziny, okres przechowywanie kopii 2 tygodnie
    e. kopie przechowywane są na macierzy dyskowej w SDC

b. Dla Centrum przetwarzania i przechowywania danych „3S Data Center S.A.":

I. Bezpieczeństwo fizyczne obiektu

1. Obiekty DC są ogrodzone, monitorowane wysokiej klasy sprzętem CCTV w trybie dzień/noc, chronione przez licencjonowaną służbę ochrony z wydzielonymi strefami bezpieczeństwa.

II. Bezpieczeństwo energetyczne i środowiskowe

1. Obiekty przyłączone są do sieci energetycznych poprzez dwóch niezależnych dostawców energii, posiadają redundantne urządzenia UPS na każdy tor zasilania, są wyposażone w agregaty prądotwórcze z możliwością produkcji energii z gazu ziemnego.
2. Zapewnione są optymalne warunki środowiskowe dotyczące temperatury i wilgotności panujących w modułach, zapewniamy również systemy gaszenia gazami obojętnymi na wypadek pożaru

III. Bezpieczeństwo infrastruktury informatycznej

1. Do budynków DC doprowadzone są przyłącza światłowodowe z minimum 3 kierunków geograficznych zapewniające ciągłość przyłącza i transmisji danych.

§ 6

Osoby odpowiedzialne za ochronę danych osobowych

1. Administrator Danych Osobowych
    a. Zgodnie z definicją zawartą w art. 7 pkt 4 Ust. „O ochronie danych osobowych" Administratorem Danych Osobowych jest firma „Dreamtec" Sp. z o.o.
    b. Obowiązkiem Administratora Danych Osobowych jest zastosować takie środki techniczne i organizacyjne, które zapewnią ochronę przetwarzania danych (zabezpieczenie przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez takie osoby, zniszczeniem, utratą lub przetwarzaniem niezgodnym z przepisami).
    c. Zarząd „Dreamtec" sp. z o.o. deklaruje zaangażowanie w prawidłowym zarządzaniu bezpieczeństwem informacji w spółce.
    d. „Dreamtec" Sp. z o.o. ma podpisane stosowne umowy z innymi firmami, które uczestniczą w procesie zapewnienia bezpieczeństwa danych.
    e. Zarząd „Dreamtec" Sp. z o.o. oświadcza, iż dołoży wszelkich starań celem zapewnienia bezpieczeństwa informacji w spółce.
    f. Zgodnie z Ust. „O ochronie danych osobowych" Art. 37. Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.

Upoważnienie musi być podpisane przez Administratora Bezpieczeństwa Informacji. Wykaz osób wraz z poziomem dostępu stanowi ***Załącznik nr 6 – Ewidencja osób upoważnionych do przetwarzania danych osobowych***

g. Zgodnie z Ust. „O ochronie danych osobowych" Art. 38. Administrator Danych Osobowych zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. W tym celu system rejestruje czas i login-y dostępu do systemu, rejestrowane są zarówno połączenia udane jak i nieudane na poziomie:
    i. warstwy programowej środowiskowej,
    ii. warstwy programowej systemowej,
    iii. warstwy programowej aplikacji.

h. Zgodnie z Ust. „O ochronie danych osobowych" Art. 39. 1. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera:
    i. imię i nazwisko osoby upoważnionej,
    ii. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
    iii. identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

i. Administrator Danych Osobowych powierza nadzorowanie zasad ochrony danych osobowych, w tym do nadawania upoważnień dostępu, Administratorowi Bezpieczeństwa Informacji.

2. Administrator Bezpieczeństwa Informacji
    a. Do uprawnień i obowiązków Administratora Bezpieczeństwa Informacji należy:
        i. nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych,
        ii. stały nadzór nad treścią Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym,
        iii. aktualizacja i modyfikacja ww. dokumentów,
        iv. czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania,
        v. udział w kontrolach prowadzonych przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych,
        vi. udzielanie odpowiedzi na zapytania kierowane do Administratora Danych Osobowych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,
        vii. nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
        viii. 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,
        ix. nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,
        x. monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.
    b. Administratorem Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony danych osobowych, o których mowa w Ust. „O ochronie danych osobowych" ust. 1 jest Pan Maciej Bojanowski (PESEL: 80120904158). ***Załącznik nr 1 – Ustanowienie Administratora Bezpieczeństwa Informacji*** oraz ***Załącznik nr 2 – Upoważnienie Administratora Bezpieczeństwa Informacji do nadawania upoważnień***

3. Administrator Systemów Informatycznych,
    a. Do uprawnień i obowiązków Administratora Systemów Informatycznych należy:
        i. nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
        ii. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
        iii. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
        iv. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych

b. Administratorem Systemów Informatycznych, nadzorującego przestrzeganie zasad ochrony systemu informatycznego, o których mowa w Ust. „O ochronie danych osobowych" ust. 1 jest Pan Robert Boehm (PESEL: ……). ***Załącznik nr 3 – Ustanowienie Administratora Systemów Informatycznych.***

4. Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie 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. ***Załącznik nr 4a – Upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę*** oraz ***Załącznik nr 4b - Upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy innej niż umowa o pracę.***
   b. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Osoby te pisemnie potwierdzają, że zachowają poufność powierzonych danych dostępowych do systemu. ***Załącznik nr 5 - Oświadczenie o zobowiązaniu się do zachowania poufności.***

§ 7

Zmiany i udostępnienie tekstu Polityki bezpieczeństwa

1. Dopuszcza się dokonywanie zmian w niniejszym dokumencie.
2. Tekst Polityki bezpieczeństwa zostanie udostępniony użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia.

01 stycznia 2017 r. Maciej Bojanowski

(data) (administrator danych osobowych)

Załącznik nr 1 – Ustanowienie Administratora Bezpieczeństwa Informacji

Niniejszym, zgodnie z art. 36a ust. 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i dyspozycją Polityki Bezpieczeństwa oraz reprezentując Administratora Danych Osobowych – „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu.

wyznaczam

Panią/Pana ……..……..
na **Administratora Bezpieczeństwa Informacji (ABI)** w firmie „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Bezpieczeństwa Informacji określone są Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia …../ …… / ……..… (dd/mm/rrrr) w firmie „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu.

DATA I PODPIS OSOBY WYZNACZONEJ
NA STANOWISKO ABI

DATA I PODPIS OSOBY REPREZENTUJĄCEJ
ADMINISTRATORA DANYCH OSOBOWYCH

Załącznik nr 2 – Upoważnienie Administratora Bezpieczeństwa Informacji do nadawania upoważnień

Niniejszym, zgodnie z dyspozycją Polityki Bezpieczeństwa oraz reprezentując Administratora Danych - „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu.

Upoważniam

Panią/Pana ……..
na **Administratora Bezpieczeństwa Informacji** w „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu do nadawania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO ABI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

Załącznik nr 3 – Ustanowienie Administratora Systemów Informatycznych

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu.

wyznaczam

Panią/Pana ……..
na **Administratora Systemów Informatycznych (ASI)** w „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia ……/ …… / …….. (dd/mm/rrrr) w „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO ASI	DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Bezpieczeństwa Informacji w „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu (dalej „ABI"), na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182) **upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych Osobowych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r., poz. 1182), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

....

Data i podpis upoważniającego Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:

1 x oryginał dokumentacja kadrowa

1 x oryginał osoba upoważniona

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Bezpieczeństwa Informacji „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu (dalej „ABI"), na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (T.j. Dz. U. z 2015 r. poz. 1309) **upoważniam:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 1309), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz odpowiedzialności cywilnej.

Upoważnienie jest ważne do odwołania.

....

Data i podpis upoważniającego Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w „Dreamtec" Sp. z o.o. z siedzibą we Wrocławiu (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych.

.....

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:

1 x oryginał dokumentacja kadrowa

1 x oryginał osoba upoważniona

……..., dnia ……..

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y ……

zamieszkała/y w……

zatrudniona/y na stanowisku ……

zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z wykonywanymi czynnościami służbowymi. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

……..

Podpis

Załącznik nr 6 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Zakres upoważnienia (uprawnienia)
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					