## 1 CEL

Celem dokumentu jest zdefiniowanie obowiązków i odpowiedzialność Dostawcy Budimex (oraz jego pracowników) w zakresie ochrony aktywów informacyjnych Budimex, do których Dostawca będzie miał dostęp i które będzie przetwarzał w toku świadczenia swoich usług.

## 2 ZAKRES

Niniejszy dokument stanowi Politykę Bezpieczeństwa Systemów Informacyjnych dla Dostawców Budimex SA, zwaną dalej „Polityką".

Zapisy zawarte poniżej regulują dwa podstawowe obszary bezpieczeństwa informacji:

- Świadczenie usług przez Dostawcę z wykorzystaniem powierzonych przez Budimex systemów informatycznych i/lub systemów informatycznych podłączanych do infrastruktury Budimex
- Świadczenie usług przez Dostawcę z wykorzystaniem jego własnych systemów informatycznych, ale przetwarzających informacje będące własnością lub, za które odpowiada Budimex (np. dane osobowe pracowników Budimex).

## 3 ODPOWIEDZIALNOŚĆ

Budimex S.A. dokłada wszelkich starań, aby zapewnić efektywne i bezpieczne funkcjonowanie przedsiębiorstwa, w celu jak najlepszego zaspokojenia potrzeb ,klientów, akcjonariuszy i pracowników Spółki. Przejawem szczególnej staranności kierownictwa Budimex S.A. jest minimalizacja ryzyka operacyjnego m.in. poprzez zapewnienie należytego poziomu bezpieczeństwa przetwarzanych aktywów informacyjnych. W tym celu, kierownictwo Budimex S.A. podjęło decyzje o wprowadzeniu w życie zasad dotyczących bezpieczeństwa informacji.

Niniejszy dokument jest wyrazem intencji Budimex w zakresie zapewnienia bezpieczeństwa aktywów informacyjnych, wynikających z przyjętej Polityki Bezpieczeństwa Informacji, aktywów udostępnianych i przetwarzanych przez Dostawców Budimex.

## 4 DEFINICJE

**Aktywa informacyjne** – informacja oraz systemy, infrastruktura, urządzenia i oprogramowanie wykorzystywane w celu przetwarzania informacji.

**Bezpieczeństwo informacji** – zapewnienie poufności, integralności i dostępności aktywów informatycznych.

**Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, bezpośrednio lub pośrednio.

**Incydent bezpieczeństwa** – niepożądane zdarzenie lub seria zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i mogą mieć negatywny wpływ na bezpieczeństwo aktywów informacyjnych.

**Informacja** - wszelka informacja, bez względu na jej formę tj.: w formie elektronicznej, zapisana w formie papierowej, przekazywana w formie ustnej.

**Informacje niejawne** – termin zdefiniowany w ustawie z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych. Oznacza informację, która wymaga ochrony przed nieuprawnionym ujawnieniem, jako stanowiącą tajemnicę państwową lub służbową, niezależnie od formy i sposobu jej wyrażenia.

**Przetwarzanie informacji -** jakiekolwiek czynności wykonywane na informacji, takie jak tworzenie, zbieranie, utrwalanie, przechowywanie, odczytywanie, zmienianie, udostępnianie, usuwanie, itd.

**Użytkownik** – każdy, kto posiada dostęp do aktywów informacyjnych Budimex – użytkownikami są pracownicy, pracownicy okresowi, konsultanci, praktykanci, klienci etc.

# 5 OPIS POSTĘPWANIA – ZASADY OGÓLNE

## 5.1 Przestrzeganie Polityki

5.1.1 Polityka, jest częścią zasad i procedur regulujących stosunki między Stronami. Polityka podlega okresowej weryfikacji. Przestrzeganie Polityki jest warunkiem zgodnego z umową świadczenia usług na rzecz Budimex.

## 5.2 Zgodność z Prawem

5.2.1 Strony muszą przestrzegać przepisów prawnych i uregulowań odnoszących się do Technologii Informatycznych.

5.2.2 Zakazane jest wykorzystywanie zasobów Systemów Informatycznych skutkujące naruszeniem prawa własności intelektualnej.

5.2.3 Instalowanie oprogramowania lub zapisywanie jakichkolwiek innych materiałów w Systemie Informatycznym powierzonym przez Budimex, które nie zostały pozyskane w sposób uprawniający Budimex do ich używania, jest sprzeczne z Polityką.

## 5.3 Prawa własności i ochrona informacji przechowywanych w formie elektronicznej.

5.3.1 Dane oraz informacje przechowywane, przetwarzane i/lub przekazywane poprzez Systemy Informatyczne należące do Budimex są pod stałą kontrolą. Kontrola obejmuje takie metody jak: przechwycenie, monitoring, wpis do dziennika zdarzeń oraz inspekcję. Celem stałej kontroli jest ochrona interesów Budimex i Dostawcy.

5.3.2 Dane oraz informacje są mieniem Budimex lub Dostawcy i wymagają traktowania jak każde inne mienie firmowe.

5.3.3 Dane oraz informacje dotyczące Budimex, przechowywane na dowolnych nośnikach lub w Systemach Informatycznych nie mogą być usuwane bez autoryzacji oraz winny być kasowane/ niszczone jedynie za zgodą i w sposób uzgodniony z właścicielem danych.

5.3.4 Dane oraz informacje powierzone Dostawcy lub wygenerowane przez niego w trakcie realizacji usług na rzecz Budimex oraz te, które są pod kontrolą Dostawcy, muszą być odpowiednio, przy użyciu dostępnych środków, chronione przez Dostawcę przed zniszczeniem, uszkodzeniem oraz nieautoryzowanym dostępem.

5.3.5 Dostawca musi przez cały czas stosować odpowiednie mechanizmy ochronne stosownie do systemów, nad którymi sprawuje kontrolę oraz w odniesieniu do danych/informacji w nich zawartych. Dostawca jest w pełni odpowiedzialny za tworzenie regularnych kopii bezpieczeństwa danych dotyczących Budimex, umieszczonych na mobilnym sprzęcie komputerowym. Dane i informacje powinny być przechowywane na przenośnych komputerach tylko w minimalnej ilości i tylko na czas niezbędny do wykonania zakresu świadczonych usług. O ile to możliwe, dane powinny być przechowywane na dyskach sieciowych.

5.3.6 Przenośny sprzęt komputerowy zawierający istotne i/lub poufne dane i informacje dotyczące Budimex musi przez cały czas być zaopatrzony w zaaprobowane przez Strony technologie blokujące nieautoryzowany dostęp.

5.3.7 Bez pisemnej zgody Budimex dane należące do Budimex nie mogą być przetwarzane lub przechowywane na sprzęcie nie należącym do Budimex (np. na komputerach domowych).

5.3.8 Okres i sposób przechowywania danych elektronicznych w Systemie Informatycznym musi być zgodny z założeniami przyjętymi dla danego systemu (retencja dokumentów).

5.3.9 Sprzęt, który nie został zatwierdzony przez Budimex, nie może zostać podłączony do Systemu Informatycznego Budimex. Podłączanie służbowych lub prywatnych telefonów komórkowych do Systemów Informatycznych Budimex jest zabronione.

5.3.10 Nie można przesyłać tajnych lub poufnych informacji za pośrednictwem Internetu. Istotne informacje (nie tajne i nie poufne) odbierane lub wysyłane przez Internet muszą być szyfrowane zgodnie z zaleceniami obowiązującej Polityki Bezpieczeństwa.

# 6 OPIS POSTĘPWANIA - ZASADY DOTYCZĄCE SYSTEMÓW UDOSTĘPNIONYCH DOSTAWCY PRZEZ BUDIMEX

## 6.1 Wykorzystanie technologii informatyczne do celów biznesowych

6.1.1 Pracownicy Dostawcy, będący użytkownikami systemów informatycznych dostarczonych przez Budimex, mogą sporadycznie wykorzystywać wspomniane zasoby do celów prywatnych. Tego typu użytkowanie nie może kolidować z wykonywaniem obowiązków służbowych i być sprzeczne z interesem Budimex.

6.1.2 Dostawca nie może wykorzystywać zasobów Systemów Informatycznych dostarczonych przez Budimex do pracy zarobkowej na rzecz innego podmiotu niż Budimex.

## 6.2 Kontrola dostępu do informacji ze źródeł elektronicznych.

6.2.1 Kontrola dostępu do informacji przechowywanych w Systemach Informatycznych Budimex jest obligatoryjna. Dla każdego Systemu przyznawana jest Użytkownikom autoryzacja dostępu w zakresie niezbędnym do wykonywania pracy.

6.2.2 Dostęp jest kontrolowany za pomocą indywidualnych identyfikatorów i haseł, jednoznacznie identyfikujących Użytkownika w Systemie Informatycznym i chroniących przed nieautoryzowanym dostępem.

6.2.3 Hasła są tworzone zgodnie z określonymi regułami, dotyczącymi ich długości, konstrukcji i częstotliwości zmian.

6.2.4 Hasła muszą być utrzymywane w tajemnicy i nie mogą zostać ujawnione innym osobom. W przypadku przekazania przez Użytkownika realizującego obowiązku Dostawcy hasła innej osobie, Dostawca pozostaje w pełni odpowiedzialny za nienaruszalność i poufność powierzonych mu informacji. Ochrona hasła leży zarówno w interesie Budimex jak i Dostawcy.

6.2.5 Użytkownik, którego identyfikator oraz hasło zostało użyte do uzyskania nieautoryzowanego dostępu do Systemu Informatycznego, zostaje uznany za tę osobę, która skorzystała z zasobów tego Systemu w sposób nieuprawniony.

6.2.6 W przypadku chwilowego opuszczenia stanowiska pracy należy zablokować konsolę komputera (np. w systemach Windows użyć klawiszy CTRL-ALT-DEL + ENTER) w celu uniemożliwienia korzystania z komputera osobom niepowołanym.

6.2.7 W przypadku dodawania nowych Użytkowników do Systemu Informatycznego wymagana jest zgoda Budimex.

6.2.8 Budimex zmieni hasło Użytkownika jedynie na podstawie żądania uprawnionej osoby, nie ujawniając dotychczasowego hasła.

6.2.9 Zabronione jest używanie Systemów Informatycznych będących w posiadaniu Budimex lub osób trzecich bez zgody osoby, która jest autoryzowana do wydawania tego typu pozwoleń.

## 6.3 Ochrona udostępnionych zasobów Systemów Informatycznych

6.3.1 Dostawca nie może modyfikować urządzeń należących do Budimex np. poprzez instalację podzespołów komputerowych, oprogramowania lub w inny sposób bez pisemnej autoryzacji odpowiedzialnego za to pracownika Budimex.

6.3.2 Dostawca powinien stale troszczyć się o powierzony mu sprzęt Budimex, a w szczególności zadbać o zabezpieczenie przed kradzieżą, zapobiegać uszkodzeniom podczas transportu lub

przenoszenia, właściwie przechowywać w odpowiedniej temperaturze oraz nie wystawiać na działanie pola magnetycznego lub złych warunków atmosferycznych.

6.3.3 Należy zachować szczególną ostrożność przy posługiwaniu się materiałami na mediach wymiennych (np. CD-ROM, itp.), które zostały utworzone lub użyte poza Systemem Informatycznym Budimex. Nie można używać mediów pochodzących z wątpliwego lub nieznanego źródła na sprzęcie należącym do Budimex. Wszelkie tego typu materiały powinny przed użyciem zostać przeskanowane programem antywirusowym i/lub przetestowane przez Biuro Informatyki Budimex.

6.3.4 Wszelkie instalacje oprogramowania na komputerach Budimex są dokonywane przez Budimex. Tylko za pisemną zgodą Budimex może zostać przeprowadzona instalacja legalnego oprogramowania do biznesowego użycia przez osoby, które nie są pracownikami Budimex.

6.3.5 Instalowanie i/ lub użycie prywatnego oprogramowania/plików na sprzęcie IT powierzonym przez Budimex jest zabronione.

6.3.6 Na powierzonym przez Budimex sprzęcie komputerowym musi być zawsze obecna i aktywna najnowsza wersja oprogramowania antywirusowego dostarczona przez Budimex. Należy przestrzegać instrukcji dostarczonych przez Budimex dotyczących prewencji antywirusowej oraz ewentualnej eliminacji wirusów, które przeniknęły do Systemu Informatycznego Budimex. W przypadku zauważenia błędnej pracy programu antywirusowego Użytkownik musi niezwłocznie zgłosić ten fakt do Biura Informatyki Budimex.

6.3.7 Wszelkie zidentyfikowane przypadki zagrożenia, naruszenia i osłabienia bezpieczeństwa Systemów Informatycznych czy funkcjonowanie nieautoryzowanego przez Budimex oprogramowania (incydenty bezpieczeństwa) muszą być niezwłocznie raportowane do Biura Informatyki Budimex.

### 6.4 Przesyłanie wiadomości drogą elektroniczną

6.4.1 Elektroniczna poczta korporacyjna Budimex, która może być udostępniona użytkownikom, za których odpowiada Dostawca, jest oficjalnym środkiem komunikacyjnym w Budimex i jest traktowana jako poczta służbowa.

6.4.2 Użytkownik, za którego odpowiedzialność ponosi Dostawca, przesyłając wiadomości drogą elektroniczną nie może przedstawiać prywatnych opinii i osądów jako stanowiska Budimex.

6.4.3 Jedynie zaaprobowane przez Budimex systemy wymiany wiadomości elektronicznych mogą być wykorzystywane na komputerach powierzonych przez Budimex.

6.4.4 Na komputerach powierzonych przez Budimex, do wysyłania lub odbierania wiadomości nie można używać zewnętrznych serwisów dostarczanych za pośrednictwem Internetu (np. Hotmail, Yahoo, WP, ONET, chat i komunikatory itp.).

6.4.5 Aby zapobiec działaniu szkodliwego oprogramowania (np. wirusów), które mogą dostać się do Systemu Informatycznego Budimex, należy natychmiast usuwać wszelką nieoczekiwaną pocztę z załącznikami od nieznanego nadawcy. Załączników z takiej wiadomości nie można otwierać.

6.4.6 Dystrybucja wiadomości e-mail w systemie poczty korporacyjnej Budimex musi być ograniczona jedynie do osób, które powinny znać ich treść lub do osób bezpośrednio związanych z treścią wiadomości. Listy dystrybucyjne nie powinny być używane z wyjątkiem sytuacji, gdy wszyscy adresaci spełniają powyższe kryteria.

6.4.7 W systemie poczty korporacyjnej Budimex, należy unikać wysyłania wiadomości z dużymi załącznikami do licznego grona osób poprzez listy dystrybucyjne. Należy używać oprogramowania kompresującego dostarczonego przez Budimex w celu ograniczenia rozmiaru dużych załączników i/lub wysłać kilka wiadomości.

6.4.8 Rozmiar powierzonej korporacyjnej skrzynki pocztowej Budimex jest ograniczony limitem. Użytkownik, za którego odpowiada Dostawca jest zobowiązany do regularnego usuwania nieaktualnych wiadomości.

## 6.5 Internet

6.5.1 W celu realizacji usług objętych umową, może być konieczne zapewnienie Dostawcy przez Budimex dostępu do Internetu. Dostęp taki podlegać będzie restrykcjom Polityki Bezpieczeństwa Informacji Budimex SA. Dostęp do Internetu z urządzeń i/ lub infrastruktury udostępnionej przez Budimex dozwolony jest jedynie poprzez dostarczone i zaaprobowane przez Budimex rozwiązania.

6.5.2 W żadnym razie Użytkownik, za którego odpowiedzialność ponosi Dostawca, nie może podłączać powierzonego mu sprzętu do Internetu lub innych sieci za pośrednictwem kabli, modemów dial-up lub bezprzewodowo bez zabezpieczeń wymaganych przez obowiązującą Politykę Bezpieczeństwa Informacji Budimex SA. Każde podłączenie do sieci komputerowej nie należącej do Grupy Budimex powierzonego przez Budimex sprzętu komputerowego musi być indywidualnie aprobowane przez Budimex.

6.5.3 Budimex zastrzega sobie prawo do monitorowania wszelkiego rodzaju połączeń z Internetem, w których udział biorą urządzenia podłączone do Systemów Informatycznych Budimex oraz do blokowania dostępu do usług i stron Internetowych, które zostaną uznane za niezgodne z Polityką Bezpieczeństwa Informacji Budimex SA.

6.5.4 Użytkownik, za którego odpowiedzialność ponosi Dostawca nie może:

- dążyć do ominięcia zabezpieczeń, kontroli dostępu lub mechanizmów filtrowania zawartości znajdujących się na bramce wyjściowej do Internetu;
- celowo zakłócać funkcjonowania sieci np. poprzez rozsyłanie wirusów komputerowych, stosowanie praktyk hakerskich oraz przesyłanie dużych ilości danych blokujących sieć i utrudniających pracę innym użytkownikom;
- ujawniać lub publikować poprzez internet tajnych lub zastrzeżonych informacji firmowych, takich jak: informacje finansowe, nowe idee lub pomysły związane z firmą, strategie i plany marketingowe, bazy danych i informacje w nich zawarte, listy klientów, kody źródłowe oprogramowania, komputerowe/sieciowe kody dostępu oraz powiązania biznesowe itp.;
- używać Internetu, poczty elektronicznej lub innych narzędzi w celu stworzenia prawnych lub kontraktowych zobowiązań bez wymaganej autoryzacji Zarządu Budimex;
- wykorzystywać zasobów w inny niewłaściwy sposób określony przez Budimex.

## 6.6 Niestosowny materiał

6.6.1 Dostawca nie może używać dostarczonego przez Budimex sprzętu komputerowego, urządzeń i pomieszczeń do oglądania, przetwarzania, tworzenia i/lub dystrybucji materiałów wśród pracowników lub kogokolwiek spoza Budimex, które zawierają treści:

- związane z dyskryminacją (rasową lub każdą inną),
- molestowaniem (seksualnym lub każdym innym),
- z pogróżkami,
- obsceniczne,
- pornograficzne,
- zniesławiające,
- nielegalne

6.6.2 Dostawca jest zobowiązany do natychmiastowego zniszczenia/usunięcia materiałów określonych w pkt. 6.6.1 otrzymanych od kogokolwiek i do wysłania żądania do nadawcy o zaniechanie tego typu praktyk w przyszłości. Należy również niezwłocznie poinformować Kierownika ds. Bezpieczeństwa Systemów IT Budimex SA o szczegółach zdarzenia, razem z podaniem adresu e-mail nadawcy, tematu i podjętych akcji.

## 7 OPIS POSTĘPWANIA - ZASADY DOTYCZĄCE SYSTEMÓW INFORMATYCZNYCH DOSTAWCY USŁUG DLA BUDIMEX

W przypadku, gdy Dostawca wykorzystuje do świadczenia usług swój system informatyczny nie będący własnością Budimex i nie podłączony do infrastruktury Budimex, poniższe wymagania stanowią minimum, aby taki system mógł być dopuszczony do dostarczania usług:

7.1 Całość oprogramowania (System Operacyjny i aplikacje) zainstalowane i użytkowane zgodnie z prawem i warunkami licencji

7.2 Każdy system operacyjny i aplikacja musi być na bieżąco weryfikowany pod kątem aktualizacji poprawek bezpieczeństwa (częstotliwość minimum 1x w miesiącu)

7.3 System , który posiada jakąkolwiek możliwość interakcji ze światem zewnętrznym (sieć komputerowa, stacja CD-ROM/DVD-ROM, USB, stacja dysków) musi koniecznie posiadać aktualne (z częstotliwością aktualizacji min 24 godzinną) i działające oprogramowanie antywirusowe. Dla systemów opartych o Windows lista dostępnych dostawców - http://windows.microsoft.com/en-US/windows/antivirus-partners#AVtabs=win7

7.4 System musi posiadać odpowiednio zaktualizowany i synchronizowany regularnie czas (w przypadku systemów z dostępem do sieci, korzystanie z serwera czasu; w przypadku systemów off-line udokumentowana synchronizacja czasu min. 1 x w miesiącu).

7.5 System musi posiadać działające i okresowo weryfikowane (testy odtworzeniowe minimum raz w roku) oprogramowanie wykonujące kopie zapasowe danych.

7.6 Całe środowisko używane w celu dostarczania usług dla Budimex musi posiadać odpowiednie zabezpieczenie logiczne i środowiskowe – zasilanie awaryjne i zabezpieczenie przed nieautoryzowanym fizycznym oraz nieautoryzowanym logicznym dostępem.

7.7 Personel obsługujący przeszkolony z zakresu obsługi systemu.

## 8 UDOKUMENTOWANE INFORMACJE

8.1 Raport z przeglądu zabezpieczeń organizacyjno – technicznych Dostawcy

## 9 ZAŁĄCZNIKI I FORMULARZE

BRAK

Data ostatniej aktualizacji: 2017-02-07