Polityka bezpieczeństwa dla systemu Luminum

§1. DEFINICJE

Ilekroć w niniejszym dokumencie jest mowa o:

1. **„Operatorze”** rozumie się przez to firmę Imbierowicz Urbaniak LUMINUM spółka komandytowa z siedzibą w Poznaniu, z adresem ul. Jesienna 21/3, 60-374 Poznań, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000799665, której dokumentacja rejestrowa jest przechowywana przez Sąd Rejonowy dla m. Poznania, Wydział VIII Gospodarczy Krajowego Rejestru Sądowego, NIP: 7792508426, REGON: 384130334.

2. **„Zbiorze danych”** - rozumie się przez to zbiór danych klientów.

3. **„Przetwarzaniu danych”** - rozumie się przez to jakiekolwiek operacje wykonywane na danych, w szczególności: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

4. **„Systemie informatycznym”** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych w systemie informatycznym Luminum stworzonym przez Technology.

5. **„Zabezpieczeniu danych w Systemie informatycznym”** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

6. **„Usuwaniu danych”** - rozumie się przez to zniszczenie danych.

7. **„Zgodzie osoby, której dane dotyczą”** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

8. **„Pracowniku”** - rozumie się pracownika Operatora.

9. **„Kliencie”** – rozumie się przez to klienta prowadzonego przez Operatora.

10. **„Sprzedaży” –** rozumie się przez to nawiązanie, ukształtowanie, zmiana treści lub rozwiązanie stosunku prawnego z klientami.

11. **„Polityce bezpieczeństwa”** - rozumie niniejszy dokument opisujący politykę bezpieczeństwa.

12. „**Ustawie”** – rozumie się przez to Ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2002, Nr. 101, poz. 926),

§2. CELE I ZASADY OCHRONY DANYCH

1. Celem wprowadzonych niniejszą Polityką bezpieczeństwa zasad jest ochrona danych przetwarzanych w Systemie informatycznym w szczególności:

a) zabezpieczenie przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzania danych, aktualizacji lub usuwania danych osobowych, wyświetlania lub drukowania zestawień,

b) ochronę zarchiwizowanych danych,

c) wprowadzenie zabezpieczeń przed dostępem osób niepowołanych do systemu informatycznego oraz do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń Pracowników, personelu pomocniczego oraz serwisu zewnętrznego,
d) monitorowanie systemu zabezpieczeń,
e) wyznaczenie zakresu obowiązków Pracowników – w zakresie bezpieczeństwa danych osobowych.

2. Operator stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Strategia ochrony danych osobowych opiera się na następujących zasadach:
a) do przetwarzania danych uprawnione są wyłącznie osoby, które zostały do tego upoważnione przez Administratora danych, każda z takich osób posiada swój identyfikator i hasło.
b) wstęp do pomieszczeń, w których przetwarzane są dane posiadają wyłącznie upoważnieni Pracownicy oraz inne osoby upoważnione przez Operatora,
c) podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania Pracowników w systemie identyfikatorów oraz haseł.
d) stosowanie kryptograficznej ochrony transmitowanych danych,
e) Infrastruktura służąca do przetwarzania danych opiera się na działaniu w klastrach, duplikacji urządzeń by minimalizować skutki ewentualnych awarii.

§3. ŚRODKI ZABEZPIECZENIA DANYCH

Wprowadza się następujące zabezpieczenia w celu danych w Systemie informatycznym:

1. Infrastruktura informatyczna wykorzystywana do świadczenia usług znajduje się w Data Center, które zapewnia następujące środki zabezpieczające:

a) Bezpieczeństwo fizyczne lokalizacji

- Budynek jest całodobowo dozorowany i monitorowany systemem kamer. Kamery obejmują polem widzenia wejścia do budynku, korytarze wewnątrz niego i wnętrze serwerowni.
- Wejście jest możliwe dla posiadających kartę wstępu.
- Wejście do serwerowni jest możliwe wyłącznie z imienną kartą wstępu.
- Drzwi do serwerowni pozostają zamknięte przez cały czas, z wyłączeniem czasu niezbędnego dla wejścia i wyjścia w celu wykonania czynności serwisowych przy serwerach.
- Wewnątrz serwerowni przebywają wyłącznie dyżurni pracownicy ochrony i służb utrzymania sieci telekomunikacyjnych.
- Serwerownia nie posiada okien, co stanowi barierę termiczną, fizyczną i optyczną.
- Podczas normalnego funkcjonowania w serwerowni nie przebywają żadne osoby trzecie.
- Szafy serwerowe są zamykane na klucz, którym dysponują jedynie upoważnieni administratorzy.

b) Bezpieczeństwo przeciwpożarowe

- Cztery systemy wczesnej detekcji pożaru Vesda, w przestrzeni serwerowej i pod podłogą techniczną.
- System gaszenia gazem technicznym Inergen.

c) Bezpieczeństwo termiczne

- Serwerownia znajduje się w przyziemiu budynku o grubych murach.
- Serwerownia jest wyposażona w:
    a. trzy niezależne komplety chillerów wysokiej mocy
    b. dwa tory zasilania w czynnik chłodniczy,
    c. szafy chłodnicze firmy Hiross Emmerson w układzie n+1.
- Obwody klimatyzacji są podłączone do generatora awaryjnego, co pozwala utrzymać klimatyzację nawet w razie zaniku napięcia na liniach energetycznych dochodzących do budynku.
- Temperatura w serwerowni jest nieustannie monitorowana przy pomocy systemu informatycznego.
- Serwery posiadają zabezpieczenie termiczne, które wyłącza serwer dla ochrony danych w razie stwierdzenia, iż temperatura osiągnęła poziom krytyczny. Ponowne włączenie serwera jest możliwe po ochłodzeniu.

d) Bezpieczeństwo łącz

- Wykorzystane są łącza od 7 niezależnych operatorów, doprowadzonych z czterech różnych stron budynku. W razie awarii któregoś z operatorów ruch jest niezwłocznie i automatycznie przełączany na drugiego operatora.
- Wykorzystane są routery, działające w trybie redundantnym, to jest w razie awarii jednego z nich drugi przejmuje na siebie obsługę sieci.

e) Bezpieczeństwo energetyczne

- Do budynku doprowadzone są dwie linie zasilające.
- Trzecie źródło zasilania stanowi generator spalinowy.
- Przełączanie zasilania następuje automatycznym układem załączania rezerwy, utrzymywanym nieustannie w podwyższonej temperaturze dla zapewnienia ciągłej gotowości do natychmiastowego działania.
- Od układu załączania rezerwy do każdej szafy są doprowadzone dwa odrębne tory zasilania, zabezpieczone osobnymi układami UPS. Urządzenia dwuzasilaczowe są wpięte każdym zasilaczem w osobne tory zasilania.

f) Bezpieczeństwo fizyczne danych na dyskach serwera

- Serwery są markowymi urządzeniami, wyposażonymi w systemy redundantne, w szczególności dotyczy to zasilaczy, wentylatorów oraz dysków.
- Macierz dyskowa serwera zbudowana w oparciu o macierz RAID 1.
- Gdyby zaszła konieczność wymiany uszkodzonego dysku, dane z napędu są kasowane przed przekazaniem dysku do naprawy przy pomocy oprogramowania służącego do zamazywania danych na dysku. Jeśli dysk nie ma być przedmiotem naprawy jest on, po logicznym usunięciu danych, niszczony fizycznie.

§4. ARCHIWIZACJA DANYCH PRZED USZKODZENIEM

1. Dane Systemu informatycznego są archiwizowane w trybie pełnym. Kopie awaryjne danych w trybie pełnym wykonywane są codziennie.