# OFERTA

**……**

**Audytu Teleinformatycznego**

dla

……..

……..

**Opracował:**

Portal Informacyjny Bezpieczny Bank Sp. z o. o.

**Informacje wstępne.**

**Podstawa przygotowania oferty.**
Niniejsza oferta Portal Informacyjny Bezpieczny Bank Sp. z o. o. dalej zwana Spółką została przygotowana po zaptaniu dla …… zwanej dalej Klientem.

**ZAKRES OFEROWANYCH USŁUG.**

Oferta swoim zakresem obejmuje całość zagadnień związanych z audytem i oceną bezpieczeństwa wykorzystywanych systemów teleinformatycznych oraz kompleksową ocenę bezpieczeństwa informacyjnego funkcjonujących u Klienta systemów teleinformatycznych.

W szczególności oferta dotyczy:

- Oceny procesu zarządzania użytkownikami
- Ocena bezpieczeństwa procesów backupu i archiwizacji.
- Oceny zabezpieczenia przed szkodliwym oprogramowaniem.
- Oceny zarządzania infrastrukturą IT.
- Oceny bezpieczeństwa innych, specyficznych rozwiązań.

Wychodząc naprzeciw potrzebom Klientów, realizacja oferty będzie poprzedzona dokładną analizą potrzeb pozwalającą na uwzględnienie specyficznych wymagań Klienta.

Wśród wymiernych korzyści, jakie w wyniku przeprowadzonego audytu bezpieczeństwa zasobów teleinformatycznych uzyskuja Klient, można wymienić:

- bezpieczeństwo realizacji celów biznesowych firmy,
- znajomość aktualnego i rzeczywistego poziomu bezpieczeństwa,
- rekomendacje pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa funkcjonujących systemów,
- możliwość planowania optymalnych inwestycji w systemy bezpieczeństwa IT,
- wiarygodność dla kontrahentów.

Badanie będzie przeprowadzone w oparciu o standardy, wytyczone:

- normami ISO 27001, ISO 27002, ISO 22301, ISO 20000,
- ITIL, COBIT,
- inne, krajowe regulacje prawne związane z zarządzaniem IT i zarządzaniem bezpieczeństwem IT.

**SZCZEGÓŁY OFERTY, ZAKRES.**

Raport audytowy.

Efektem audytu bezpieczeństwa będzie raport zawierający informacje zebrane podczas działań audytowych, w tym wyniki testów podatności oraz zalecenia i dobre praktyki niezbędne do sprawnego rozwiązania napotkanych problemów.

Szczególną uwagę zamierzamy poświęcić następującym zagadnieniom:

- proces nadawania i odbierania uprawnień,
- skuteczność wykonywania kopii zapasowych,
- zabezpieczenia nośników wymiennych,
- zabezpieczenia przed wirusami,
- zabezpieczenia przed możliwością nieautoryzowanych instalacji oprogramowania,
- skuteczność instrukcji serwisowych,
- konfiguracja urządzeń sieciowych,
- zarządzanie aktualizacjami oprogramowania,

oraz planujemy i proponujemy realizację:

- testów podatności serwerów,
- testów podatności usług hostingowych,

W przypadku niezgodności krytycznych mających poważny wpływ na bezpieczeństwo przetwarzanych danych, audytor natychmiast poinformuje o tym wyznaczoną wcześniej osobę,

Po przeprowadzeniu testów podatności, wyniki zostaną bez zbędnej zwłoki przekazywane pracownikom Działu IT.

W ostatnim dniu audytu zostanie zorganizowane spotkanie poświęcone prezentacji wyników przeprowadzonych działań.

Ostateczna forma raportu przekazana będzie w formie drukowanej.

## Ważna Informacja Dodatkowa

Ważne aby podkreślić, że na etapie wstępnym, podstawowym problemem jest ustalenie z jakimi rozwiązaniami w zakresie IT będziemy mieć do czynienia. Stąd propozycja wstępnego spotkania, zwanego w terminologii audytorskiej: Preliminary Survey

## Ocena procesu zarządzania użytkownikami

Ocena procesu zarządzania użytkownikami wykonanie analizy procesów uzyskania dostępu do zasobów wewnętrznych, zmiany uprawnień, zawieszania i odbierania dostępówSprawdzane są następujące parametry:

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Potencjalne podatności
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane ze stosowanymi rozwiązaniami lub dotyczące implementacji nowych.

## Ocena bezpieczeństwa procesów backupu i archiwizacji

Ocena bezpieczeństwa procesów backupu i archiwizacji obejmuje wykonanie analizy architektury przyjętego rozwiązania, sposobów wykonywania kopii zapasowych i zabezpieczenia nośników oraz kwestie formalne związane z lokalizacjami i czasem przechowywania kopii archiwalnych.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Potencjalne podatności
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane ze stosowanymi rozwiązaniami lub dotyczące implementacji nowych.

## Ocena zabezpieczenia przed szkodliwym oprogramowaniem

Ocena bezpieczeństwa  obejmuje wykonanie analizy ryzyka funkcjonujących rozwiązań w tym zakresie.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Potencjalne podatności
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane ze stosowanymi rozwiązaniami lub dotyczące implementacji nowych.

## Ocena zarządzania infrastrukturą IT

Ocena zarządzania infrastrukturą IT obejmuje

- Sprawdzenie zgodności ze standardami bezpieczeństwa i dobrymi praktykami branżowymi.
- Analiza urządzeń i systemów sieciowych.
- Analiza zabezpieczeń oprogramowania.

- Analiza metod aktualizacji oprogramowania.
- Testowanie infrastruktury bezpieczeństwa.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Potencjalne podatności
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane ze stosowanymi rozwiązaniami lub dotyczące implementacji nowych.

Po zakończeniu prac związanych z oceną bezpieczeństwa tworzony jest raport zawierający ocenę ryzyka, opis ewentualnych luk w bezpieczeństwie, propozycje rozwiązania problemów oraz rekomendacje w celu podniesienia bezpieczeństwa.

**Oferta**

Obecnie Spółka wraz z Partnerem ASCOMP S.A. z którym współpracuje od 2000 roku dostarcza swoim Klientom kompletną ofertę produktów i usług w następujących obszarach:

- Bezpieczeństwo transmisji danych
- Serwery i Storage
- Sprzęt aktywny
- Systemy radiowe
- Oprogramowanie
- Unified Communications
- Infrastruktura Data Center
- Audyt Infrastruktury Teleinformatycznej

Partnerzy firmy ASCOMP S.A. to najbardziej liczące się firmy IT na świecie. Należą do nich przede wszystkim:

## Kompetencje

Kancelaria i ASCOMP SA kładzie silny nacisk na szkolenia, egzaminy i certyfikaty swoich audytorów i inżynierów. Są szkoleni przez wiodących na świecie producentów sprzętu IT, co pozwala im dzielić się z Klientami wiedzą o najnowszych produktach i najbardziej zaawansowanych rozwiązaniach.

Wieloletnie doświadczenia z wdrożeń połączone z szeroką i specjalistyczną wiedzą skutkują szybką analizą problemów sieci, doborem właściwych rozwiązań, które usprawnią pracę administratorów.

***Piotr Krajewski***

***Adwokat**, Radca prawny absolwent Uniwersytetu Jagiellońskiego w Krakowie, były pracownik Prokuratury Rejonowej Kraków – Śródmieście w Krakowie, aplikacja prokuratorska, prawnik w Krakowskim Domu Maklerskim S.C. w Krakowie, Były Dyrektor Operacyjny w Banku BPH SA w Krakowie; wieloletnie doświadczenie w zakresie obsługi prawnej szeregu instytucji rynku finansowego. Ekspert Rady Bankowości Elektronicznej przy Związku Banków Polskich. Ekspert Instytutu Copernicus. Honorowy Prezes ACFE Polska.*

*Specjalizacja:*

*prawo gospodarcze, ze szczególnym uwzględnieniem prawa bankowego i publicznego obrotu papierami wartościowymi, prawo karne, ze szczególnym uwzględnieniem problematyki przestępczości w obrocie gospodarczym oraz przestępstw finansowych w bankowości i podmiotach gospodarczych, bezpieczeństwo prowadzenia biznesu – projektowanie i opiniowanie rozwiązań ograniczających straty finansowe, przeciwdziałanie wprowadzeniu do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł, ryzyko operacyjne podmiotów gospodarczych, także instytucji finansowych, zarządzanie ciągłością prowadzenia biznesu, **Business Continuity Management,** ryzyko utraty reputacji oraz ryzyko strat powstałych w wyniku działań nieuczciwych klientów i pracowników, zagadnienia związane z bezpieczeństwem systemów teleinformatycznych, procedury, rozwiązania, standardy, postępowania wyjaśniające, audyt bezpieczeństwa prawnego, zagadnienia związane z **Compliance** w zakresie informacji poufnych i zgodności przestrzegania przepisów w podmiotach gospodarczych, ochrona danych osobowych i zarządzanie danymi osobowymi w podmiotach gospodarczych, prawo cywilne ze szczególnym uwzględnieniem prawa spadkowego, bardzo dobra znajomość zagadnień IT,*

*język angielski.*

**Mariusz Podolski**

**Starszy Audytor**

Audyt wszystkich obszarów działalności, zwłaszcza związanych z Zarządzaniem Ryzykiem, Operacjami;

Bezpieczeństwem, Compliance oraz usługami wewnętrznymi i zarządzaniem projektami;

- Postępowania wyjaśniające, zwłaszcza w zakresie głównej odpowiedzialności;

- Tworzenie i rozwój metodologii oceny ryzyka oraz doradztwo w zakresie zarządzania ryzykiem;

- Sporządzanie analiz ryzyka oraz wieloletnich planów działania (około 40 tematów z cz. 1-3 lata);

- Odpowiedzialność za sporządzenie planów rocznych, szczegółowych i wytycznych; Kontrole jakości i

efektywności procesów i procedur oraz konsultacje w tym zakresie;

- Kontrole zakresie ryzyka zgodności;

- Audyt kooperantów w zakresie bezpieczeństwa danych i bezpieczeństwa ciągłości działania;

- Postępowania wyjaśniające w sprawach związanych z zakresem głównej odpowiedzialności;

- Udział w licznych projektach (w tym międzynarodowych, Bazylea II, SOX, ryzyko operacyjne i inne);

- Sporządzanie raportów i analiz w powyższych tematach;

- Współpraca międzynarodowa z BACA (Austria), HVB (Niemcy), UCI (Włochy), GE (global).

**Bartłomiej Kilanowicz**

**Audytor Systemów Bezpieczeństwa i Systemów Sieciowych**

Audyt systemów teleinformatycznych z zakresu rozwiązań bezpieczeństwa, switchingu, routingu oraz sieci bezprzewodowych
- Certyfikaty Cisco i Juniper z zakresu rozwiązań sieciowych i bezpieczeństwa,
- Weryfikacja poprawności działania systemów sieciowych i bezpieczeństwa
- Określanie celów strategicznych dla działania systemów sieciowych i bezpieczeństwa
- Projektowanie sieci przewodowych i bezprzewodowych
- Projektowanie systemów zabezpieczających sieci kampusowe i centra danych
- Implementacja systemów sieciowych i bezpieczeństwa
- Wsparcie techniczne klientów korporacyjnych w administracji rozwiązań sieciowych i bezpieczeństwa

## 1. Zakres oferty

Oferta swoim zakresem obejmuje całość zagadnień związanych z audytem i oceną bezpieczeństwa wykorzystywanych systemów teleinformatycznych oraz kompleksową współpracę w celu osiągnięcia i utrzymania właściwego poziomu bezpieczeństwa systemów teleinformatycznych.

W szczególności oferta dotyczy:

- Inwentaryzacji sieci.
- Oceny bezpieczeństwa sieci przewodowej (Ethernet)
- Ocena bezpieczeństwa sieci bezprzewodowych.
- Oceny bezpieczeństwa punktów styku z sieciami zewnętrznymi (np. Internet).
- Oceny bezpieczeństwa aplikacji udostępnianych w Internecie.
- Oceny bezpieczeństwa aplikacji wykorzystywanych lokalnie.

Wychodząc naprzeciw potrzebom Klienta, oferta jest poprzedzona dokładną analizą potrzeb pozwalającą na uwzględnienie specyficznych wymagań Klienta.

Wśród wymiernych korzyści, jakie w wyniku przeprowadzonej oceny bezpieczeństwa zasobów teleinformatycznych uzyskuje Klient, można wymienić:

- bezpieczeństwo realizacji celów biznesowych Klienta,
- znajomość aktualnego i rzeczywistego poziomu bezpieczeństwa,
- rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów,
- możliwość planowania optymalnych inwestycji w systemy bezpieczeństwa IT,
- wiarygodność dla Klientów oraz kontrahentów .

## 2. Inwentaryzacja sieci

Inwentaryzacja sieci ma na celu sprawdzenie topologii sieci i jej analizę z punktu widzenia wydajności i odporności na awarie. Analizowana jest konfiguracja aktywnych urządzeń sieciowych (przełączniki, rutery, oraz wszystkie urządzenia na ścieżce danych ze skonfigurowanymi funkcjonalnościami rutingu i/lub switchingu).

Przeprowadzenie inwentaryzacji sieci ma na celu dostarczenie informacji o rzeczywistej topologii sieci i potencjalnych zagrożeniach z niej wynikających. Jej częścią jest również przedstawienie zaleceń, których zastosowanie pozwoli na poprawę pracy sieci lub zwiększenie jej odporności na awarie.

Inwentaryzacja sieci może obejmować:

- Analizę topologii sieci
- Analizę konfiguracji urządzeń aktywnych
- Analiza teoretycznej wydajności i rzeczywistego wykorzystania sieci (UWAGA: zależy od dostępnej funkcjonalności urządzeń aktywnych)
- Analiza podatności sieci na awarie poszczególnych urządzeń (możliwe przeprowadzenie testów)
- Analizę zgodności konfiguracji dostępu do urządzeń aktywnych z założeniami ujętymi w Polityce Bezpieczeństwa firmy.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Mapy sieci obrazujące jej topologię w warstwie 2. i 3. modelu OSI/ISO
- Analizę wydajności sieci dla wykorzystywanych w niej usług (QoS)
- Potencjalne podatności na nieautoryzowany dostęp do urządzeń aktywnych
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane z rekonfiguracją stosowanych systemów lub implementacji nowych.

Przeprowadzona inwentaryzacja umożliwia wskazanie potencjalnych problemów wynikających z:

- Niedostosowania topologii sieci do wymagań wydajnościowych i odporności sieci
- Wykorzystania urządzeń nieodpowiedniej klasy
- Błędów konfiguracyjnych
- Znanych podatności wykorzystywanych urządzeń aktywnych

## 3. Ocena bezpieczeństwa sieci przewodowej

Ocena bezpieczeństwa sieci przewodowej obejmuje wykonanie analizy ryzyka uzyskania dostępu do sieci przewodowej oraz możliwości uzyskania podwyższonych uprawnień przez znanych użytkowników.

Sprawdzane są następujące parametry:

- Zabezpieczenia stosowane na portach sieciowych dostępnych w przestrzeniach otwartych (np. sale konferencyjne) i objętych budynkową kontrolą dostępu.
- Sposoby uwierzytelniania pracowników i gości.
- Weryfikacja stanu bezpieczeństwa urządzeń podłączanych do sieci.
- Podział użytkowników sieci na grupy, sprecyzowanie uprawnień dla każdej z grup i poprawność autoryzacji użytkowników.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Potencjalne podatności
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane z rekonfiguracją stosowanych systemów lub implementacji nowych.

## 4. Ocena bezpieczeństwa sieci bezprzewodowych

Ocena bezpieczeństwa sieci bezprzewodowej obejmuje wykonanie analizy architektury przyjętego rozwiązania, sposobów zabezpieczenia integralności i poufności transmisji, oraz kwestie uwierzytelniania i autoryzacji użytkowników.

Sprawdzeniu podlegają następujące aspekty:

- Analiza architektury sieci z punktu widzenia zarządzania infrastrukturą bezprzewodową oraz ścieżek transmisji danych.
- Sprawdzenie wykorzystywanych algorytmów szyfrowania transmisji.
- Pokrycie lokalizacji sygnałem radiowym, pomiary mocy sygnału oraz dostępnej przepustowości sieci. Analiza propagacji sygnału na obszarach niepożądanych (np. inne piętra, parkingi, itd.)
- Ocena zagrożeń związanych z fizycznym dostępem do urządzeń transmisyjnych.
- Sposoby uwierzytelniania pracowników i gości.
- Weryfikacja stanu bezpieczeństwa urządzeń podłączanych do sieci.
- Podział użytkowników sieci na grupy, sprecyzowanie uprawnień dla każdej z grup i poprawność autoryzacji użytkowników.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Mapę sieci bezprzewodowej z uwzględnieniem mocy sygnału i możliwych do osiągnięcia przepustowości sieci oraz umiejscowienia urządzeń transmisyjnych
- Potencjalne podatności
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane z rekonfiguracją stosowanych systemów lub implementacji nowych.

## 5. Oceny bezpieczeństwa punktów styku z sieciami zewnętrznymi

Ocena bezpieczeństwa obejmuje wykonanie analizy ryzyka wszystkich urządzeń pracujących na styku sieci wewnętrznej z Internetem lub innymi sieciami publicznymi (np. PSTN, GSM). Analiza może obejmować również dostęp realizowany za pomocą połączeń VPN dla pracowników i lokalizacji zdalnych.

Oceniane są zagrożenia wynikające z dostępu pracowników do Internetu. Analizie poddaje się urządzenia sieciowe, firewalle, serwery proxy, system antywirusowy, urządzenia do filtracji treści, VPN itp.

Po zakończeniu prac związanych z oceną bezpieczeństwa tworzony jest raport zawierający ocenę ryzyka, opis ewentualnych luk w bezpieczeństwie, propozycje rozwiązania problemów oraz rekomendacje w celu podniesienia bezpieczeństwa.

Ocena bezpieczeństwa punktów styku z sieciami zewnętrznymi między innymi obejmuje:

- Zgodność ze standardami bezpieczeństwa.
- Inwentaryzację zasobów.
- Analiza urządzeń obsługujących warstwę sieci.
- Analiza urządzeń zabezpieczających punkty styku.
- Wyszukiwanie podatności.
- Audyt konfiguracji.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Potencjalne podatności w miejscach styku z sieciami zewnętrznymi wynikające z wykorzystywanych systemów bezpieczeństwa (lub ich braku) oraz ich konfiguracji
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane z rekonfiguracją stosowanych systemów lub implementacji nowych.

## 6. Oceny bezpieczeństwa aplikacji udostępnianych lokalnie i w Internecie

Ocena bezpieczeństwa aplikacji udostępnianych w Internecie i/lub lokalnie obejmuje analizę topologii i konfiguracji infrastruktury sieciowej i systemów bezpieczeństwa wykorzystywanych do świadczenia usług będących przedmiotem audytu.

Ocena bezpieczeństwa aplikacji obejmuje:

- Sprawdzenie zgodności ze standardami bezpieczeństwa i dobrymi praktykami branżowymi.
- Inwentaryzację zasobów.
- Analiza urządzeń obsługujących warstwę sieci.
- Analiza urządzeń i systemów bezpieczeństwa.
- Analiza zabezpieczenia dostępu do badanych aplikacji.
- Testowanie infrastruktury bezpieczeństwa.

Wynikiem prac jest stworzenie raportu zawierającego:

- Opis przeprowadzonych prac
- Potencjalne podatności aplikacji wynikające z wykorzystywanych systemów bezpieczeństwa (lub ich braku) oraz ich konfiguracji
- Analizę ryzyka wynikającego z wykrytych potencjalnych podatności
- Rekomendacje i zalecenia związane z rekonfiguracją stosowanych systemów lub implementacji nowych.

***Harmonogram prac do uzgodnienia. Zakładamy, że wykonanie powyższych prac u Klienta potrwa ok. 5 dni roboczych oraz przygotowanie raportu potrwa do 21 dni roboczych, w zależności od zakresu zleconych prac (analiza przez ekspertów zebranych informacji, dokumentów i regulacji) oraz rozmów z osobami odpowiedzialnymi u Klienta za poszczególne podobszary.***

**Wymiana informacji.**

***Dokumenty zostaną dostarczone w formie elektronicznej w formacie MS Office na nośniku CD lub DVD. Wymiana informacji istotnych dla wykonania zlecenia następować będzie wyłączenie w formie pisemnej. Za formę pisemną uznaje się również formę fax`u i e-mail`a podanych w umowie. W celu zapewnienia prawidłowego wykonania zlecenia wyznacza się osoby odpowiedzialne po stronie Zleceniodawcy i Zleceniobiorcy za koordynację działań związanych z jego przebiegiem.***

1. **Wynagrodzenie.**

Proponowane estymowane wynagrodzenie za przeprowadzenie projektu wynosi, **od 40 000,00 zł (słownie: czterdziestu tysięcy zł 00/100) do 90 000,00 zł (słownie dziewiedziesieciu tysięcy złoty 00/100) netto.**

Przy założeniu, że nakład pracy będzie obejmował standardowy zakres prac, a ilość godzin nie przekroczy ilość godzin pomnożonych przez zaproponowane stawki poniżej.

Powyższe wynagrodzenie zastało skalkulowane w oparciu o stawki Spółki zawarte w poniższej tabeli. (Po przekroczeniu ilości godzin wynikających z zaproponowanego wynagrodzenia stosuje się stawki o 10% wyższe).

| **Stanowisko** | **Stawka netto (za godzinę)/(za dzień)** |
|---|---|
| Prezes/Dyrektor Zarządzajacy/Dyrektor/Konsultant | **450,00 zł/3000,00 zł** |
| Menedżer/Radca prawny/Adwokat/ | **300,00 zł/2000,00 zł** |
| Ekspert | **250,00 zł/1600,00 zł** |

2. **Płatności.**

Platne w 50 % w dniu podpisania umowy zlecenia oraz 50 % 14 dni po zakończeniu projektu i jego wdrożeniu na podstawie faktury + podatek VAT zgodnie z obowiązującymi przepisami stawkami. Zleceniodawca upoważni Zleceniobiorcę do wystawiania faktur VAT bez jego podpisu. Wynagrodzenie będzie powiększane o wysokość kosztów bezpośrednich, niezbędnych do wykonania zlecenia, w szczególności udokumentowanych kosztów tłumaczeń, dojazdów i noclegów, delegacji, na które zgodę wyrazi Zleceniodawca.

Wynagrodzenie obejmuje przygotowanie projektu i przeprowadzenie projektu zgodnie z zamowieniem Oferta ważna jest 30 dni.

3. **Klauzula o poufności oferty.**

Niniejszy dokument stanowi tajemnicę handlową Spółki i podlega następującym zastrzeżeniom:

- jest przeznaczony wyłącznie dla Klienta do wiadomości osób zaangażowanych w zagadnienia objęte niniejszą ofertą;

- udostępnianie go w jakiejkolwiek formie innym osobom bez Spółki jest zabronione.

**4. Uwagi. Bezpieczeństwo Informacji.**

Wykorzystanie w biznesie nowoczesnych technologii niesie za sobą oczywiste korzyści. Warto jednak zdawać sobie sprawę również z potencjalnych zagrożeń związanych z bezpieczeństwem informacji, takich jak włamania, kradzież danych, utrata danych, nieuprawniona modyfikacja czy też ataki z wykorzystaniem złośliwego oprogramowania. Świadome zarządzanie przedsiębiorstwem to między innymi zapewnienie ochrony newralgicznych danych, których utrata , nieuprawniona modyfikacja, bądź wyciek mogą mieć dla firmy negatywne skutki.

Nasz Dział Audytu Bezpieczeństwa Informacji to grupa ekspertów - specjalistów z wieloletnim doświadczeniem w zakresie bezpieczeństwa informacji. Nasze doświadczenie, zdobyte

w różnorodnych projektach i pracach konsultingowych pozwala nam na podjęcie współpracy niezależnie od skali przedsięwzięcia.

Obszary, w których się specjalizujemy to:

Zgodność z przepisami i regulacjami.

Bezpieczeństwo urządzeń występujących w środowisku użytkownika końcowego.

Bezpieczeństwo rozwiązań sieciowych.

Bezpieczeństwo usług serwerowych.

Bezpieczeństwo aplikacji .

Bezpieczeństwo Informacji i Ochrona Danych

Metodyka, którą opracowaliśmy gwarantuje rozsądny dobór zakresu usług i rozwiązań opartych na sprawdzonych standardach. Potrafimy oszacować ryzyko związane z utratą danych, co pozwala naszym Klientom uniknąć znaczących kosztów oraz umożliwia zaplanowanie wydatków na bezpieczeństwo zgodnie ze stanem faktycznym oraz realnymi potrzebami.

Nasza oferta w zakresie bezpieczeństwa informacji obejmuje między innymi:

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI/ISMS) zgodnie

z normą PN-ISO/IEC 27001.

Opracowanie polityki bezpieczeństwa lub wybranych procedur.

Audyt zarządzania bezpieczeństwem informacji.

Audyt planów ciągłości działania.

Audyt zgodności z obowiązującymi regulacjami np. z Ustawą o ochronie danych osobowych.

Audyt bezpieczeństwa systemów informatycznych.

Audyt bezpieczeństwa aplikacji.

Audyt powdrożeniowy.

Audyt licencji oprogramowania.

Testy penetracyjne.

Ocena i dobór rozwiązań infrastrukturalnych.

Warsztaty i szkolenia.

Doradztwo w zakresie ochrony danych podlegających ochronie.

Doradztwo i wdrożenia w zakresie systemów backupu danych.

Doradztwo w zakresie szyfrowania wrażliwych danych.

Odtwarzanie poawaryjne danych i systemów.

Wykrywanie i zapobieganie inwigilacji elektronicznej

Wszystkie nasze działania oparte są na oficjalnych metodologiach i zaleceniach :

Norm ISO/IEC 27001: 2005 i ISO/IEC 17799:2005.

Ustawy o ochronie danych osobowych.

Ustawy o ochronie informacji niejawnych.

Ustawy o ochronie baz danych.

Rozporządzenia Rady Ministrów o wymogach systemów IT przetwarzających dane podlegające ochronie.

Rozporządzenia MSWiA o bezpieczeństwie danych osobowych.

Innych obowiązujących dobrych praktykach dotyczących bezpieczeństwa informacji.

**Uwagi.**

Wszystkie nasze działania oparte są na oficjalnych metodologiach i zaleceniach:

- Norm ISO/IEC 27001: 2005 i ISO/IEC 17799:2005.
- Ustawy o ochronie danych osobowych.
- Ustawy o ochronie informacji niejawnych.
- Ustawy o ochronie baz danych.
- Rozporządzenia Rady Ministrów o wymogach systemów IT przetwarzających dane podlegające ochronie.
- Rozporządzenia MSWiA o bezpieczeństwie danych osobowych.
- Innych obowiązujących dobrych praktykach dotyczących bezpieczeństwa informacji.

**Referencje.**

NTT system S. A. z Warszawy (Jacek Kozubowski).

IGEPA Polska Sp. z o. o. z Krakowa (Dorota Gajdzińska).

FCA Sp. z o. o. z Krakowa (Andrzej Szymowski).

PHU „LOBOS" Sp. z o. o. z Krakowa (Marcin Łobos).

PH „LOBOS" Sp. J. z Krakowa (Adam Łobos).

SUPO CERBER Sp. z o. o. z Krakowa (Józef Seweryn).

ZIKO Spółka z ograniczoną odpowiedzialnością z Krakowa (Marzena Karcz).

EC Sybil Tech Sp. z o. o. (Marek Oliszewski).

FEV Motorentechnik GmbH, Aachen, Germany (Michael Voβ).

FEV Polska Sp. z o. o. z Krakowa (Filip Chełmiński, Hermana Ecker).

SPACECOM Ltd, Ramat Gan, Izrael (David Pollack).

Krakowski Dom Maklerski IDM SA z Krakowa.

Comp S. A. z Warszawy (Andrzej Haliniak).

LEX – Kancelaria Odszkodowawcza Beata Jarzyna Sp. K. z Krakowa (Krzysztof Jarzyna).

UPM – KYMMENE Sp. z o. o. z Warszawy (Heikki Taskinen, Andre Faust).

Korporacja Budowlana DORACO Sp. z o. o. z Gdańska (Karol Zduńczyk).

Kompania Piwowarska S. A. z Poznania (Bartłomiej Stachowiak).

Deloitte Advisory Sp. z o. o. z Warszawy (Romuald Paprzycki).

R.R. Donnelley Europe Sp. z o. o, z Krakowa (Jan Przepiór).

TUiR/TUnŻ Warta SA z Warszawy ( Piotr Piasecki ).

Bank DnB Nord S. A. z Warszawy (Adam Grześkiewicz).

Fundusz Pożyczkowy Województwa Świętokrzyskiego Sp. z o. o. z Kielc (Krzysztof Zaremba).

Alior Bank S.A. z Warszawy (Dariusz Polaczyk).

Bank BPH S.A. z Warszawy (Paweł Bandurski).

Gospodarczego Banku Spółdzielczego w Barlinku (Zbigniew Wielgosz).

**ASCOMP SA**


GOODYEAR
DĘBICA
bumar amunicja
FAKRO
OKNOPLAST
Śnieżka
ORLEN
colig
Nestlé
CPP
Bank BPH
Nordea
BRE BANK SA
Raiffeisen BANK
inteligo
Komisja Nadzoru Finansowego
ICN Polfa Rzeszów S.A.
VALEANT
ADAMED
Polfa PABIANICE
FERRERO
MOTOROLA
upc
EXTEL
T-Mobile
netia
Polkomtel S.A.
ENION
PGE
astanet
multimedia
KATOWICE
MAŁOPOLSKI
Pałac Kultury i Nauki Warszawa
IKEA
LEROY MERLIN
MOTA-ENGIL
AGH
Biblioteka Jagiellońska
UP

**Termin oferty**

Oferta jest ważna przez 30 dni.

Z poważaniem

Piotr Krajewski – Adwokat

Warszawa, dnia 14 czerwca 2017 r

**Osoby upoważnione do kontaktów ze strony Spółki.**

PIOTR KRAJEWSKI – Prezes Zarządu – Adwokat – Ekspert ds. bezpieczeństwa transakcji elektronicznych Rady Bankowości Eleltronicznej Związku Banków Polskich

Tel: +48 605610623 e-mail: piotr.krajewski@bezpieczny-bank.eu

**Nazwa i siedziba oferenta.**

Piotr Krajewski Prezes Zarządu

e - mail: piotr.krajewski@bezpieczny-bank.eu

tel. kom./mobile +48605610623

**Portal Informacyjny Bezpieczny Bank Sp. z o. o.**

**ul. Portowa 22A, 30 - 709 Kraków,**

tel. +48 12 294 25 80, fax. +48 12 294 25 81,

www.bezpieczny-bank.eu

NIP: 6751482480, REGON: 122691188, KRS 0000438113

Sąd Rejonowy dla Krakowa –Śródmieścia w Krakowie,

XI Wydział Gospodarczy