**Załącznik nr 1 do zapytania ofertowego**

## Szczegółowy opis przedmiotu zamówienia

**„Przeprowadzenie audytów zgodności z wymaganiami KRI w Starostwie Powiatowym w Aleksandrowie Kujawskim i jednostkach organizacyjnych powiatu" w ramach projektu grantowego pn. „Cyberbezpieczny samorząd" współfinansowanego ze środków Unii Europejskiej w ramach programu: FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC), Priorytet II - Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, z podziałem na trzy części:**

## Część I – audyt KRI w Starostwie Powiatowym w Aleksandrowie Kujawskim w 2024 roku

1. **Zakres i przedmiot audytu godności z wymaganiami KRI obejmuje przegląd systemów pod kątem zarządzania bezpieczeństwem informacji, umożliwiających realizację i egzekwowanie działań:**
   1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
   2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
   3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
   4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
   5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
   6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
   7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
      a) monitorowanie dostępu do informacji,
      b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
      c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
   8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
   9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
    a) dbałości o aktualizację oprogramowania,
    b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
    c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
    d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
    e) zapewnieniu bezpieczeństwa plików systemowych,
    f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
    g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
    h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
15) rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

## 2. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do:

1. dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, zgodnie z § 19 rozporządzeniem Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 773),
2. opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami. Dokumentacja poaudytowa (raport) ma być przygotowana zgodnie z zasadami dostępności cyfrowej dokumentów tekstowych opisanymi na stronie https://www.gov.pl/web/dostepnosc-cyfrowa/jak-zwiekszyc-dostepnosc-cyfrowa-dokumentow-tekstowych oraz oznaczona pełnokolorowym znakiem Funduszy Europejskich, znakiem barw RP i znakiem UE lub znakiem monochromatycznym (zgodnie z Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji).
3. realizacji przedmiotu zamówienia w siedzibie zamawiającego.

## 3.Szczegółowe parametry zamówienia:

## NAZWA JEDNOSTKI – Starostwo Powiatowe w Aleksandrowie Kujawskim

a) Ilość pracowników: 69
b) Ilość lokalizacji: 2
c) Ilość serwerów fizycznych: 5

## Część II – audyt zgodności z wymaganiami KRI w Starostwie Powiatowym w Aleksandrowie Kujawskim i jednostkach organizacyjnych w 2025 roku

### 1.Zakres i przedmiot zgodności z wymaganiami audytu KRI obejmuje przegląd systemów pod kątem zarządzania bezpieczeństwem informacji, umożliwiających realizację i egzekwowanie działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

d) zagrożenia bezpieczeństwa informacji,
e) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
f) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

d) monitorowanie dostępu do informacji,
e) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
f) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

i) dbałości o aktualizację oprogramowania,
j) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
k) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
l) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
m) zapewnieniu bezpieczeństwa plików systemowych,
n) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

o) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

p) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
15) rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

## 2.W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do:

1. dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, zgodnie z § 19 rozporządzeniem Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 773),
2. opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami. Dokumentacja poaudytowa (raport) ma być przygotowana zgodnie z zasadami dostępności cyfrowej dokumentów tekstowych opisanymi na stronie https://www.gov.pl/web/dostepnosc-cyfrowa/jak-zwiekszyc-dostepnosc-cyfrowa-dokumentow-tekstowych oraz oznaczona pełnokolorowym znakiem Funduszy Europejskich, znakiem barw RP i znakiem UE lub znakiem monochromatycznym (zgodnie z Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji).
3. realizacji przedmiotu zamówienia w siedzibie zamawiającego.

## 3.Szczegółowe parametry zamówienia:

1. **NAZWA JEDNOSTKI – Starostwo Powiatowe w Aleksandrowie Kujawskim, ul. Słowackiego 8, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 69
   b) Ilość budynków: 2
   c) Ilość serwerów fizycznych: 5
2. **NAZWA JEDNOSTKI – Zespół Szkół Nr 1 Centrum Kształcenia Praktycznego w Aleksandrowie Kujawskim, ul. Wyspiańskiego 4, 87-700 w Aleksandrów Kujawski**
   a) Ilość pracowników – 87 (w tym 67 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 0
3. **NAZWA JEDNOSTKI – Zespół Szkół Nr 2 im. Mjra H. Dobrzańskiego „Hubala" w Aleksandrowie Kujawskim, ul. Sikorskiego 2 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 79 ( w tym 69 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 1
4. **NAZWA JEDNOSTKI – Liceum Ogólnokształcące im. Stanisława Staszica w Ciechocinku, ul. Kopernika 1, 87-720 Ciechocinek**
   a) Ilość pracowników: 33 ( w tym 27 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 1
5. **NAZWA JEDNOSTKI – Szkoła Podstawowa Specjalna nr 4 im. Jana Pawła II w Aleksandrowie Kujawskim, ul. Strażacka 22, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 59 (w tym 48 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 0

6. **NAZWA JEDNOSTKI – Placówka Socjalizacyjna w Aleksandrowie Kujawskim, ul. Wyspiańskiego 4, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 15
   b) Ilość serwerów fizycznych: 1
7. **NAZWA JEDNOSTKI – Dom Pomocy Społecznej w Zakrzewie, ul. Inowrocławska 20, 87-707 Zakrzewo**
   a) Ilość pracowników: 79
   b) Ilość serwerów fizycznych: 1
8. **NAZWA JEDNOSTKI – Poradnia Psychologiczno - Pedagogiczna w Aleksandrowie Kujawskim, ul. Sikorskiego 3, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 18 ( w tym 13 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 1
9. **NAZWA JEDNOSTKI – Powiatowe Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim, ul. Sikorskiego 3, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 13
   b) Ilość serwerów fizycznych: 1
10. **NAZWA JEDNOSTKI – Powiatowy Urząd Pracy w Aleksandrowie Kujawskim, ul. Przemysłowa 1, 87-700 Aleksandrów Kujawski**
    a) Ilość pracowników: 32
    b) Ilość serwerów fizycznych: 2
11. **NAZWA JEDNOSTKI – Zarząd Dróg Powiatowych w Aleksandrowie Kujawskim, Odolion ul. Szosa Ciechocińska 22, 87-700 Aleksandrów Kujawski**
    a) Ilość pracowników: 10
    b) Ilość serwerów fizycznych: 0

## Część III – audyt zgodności z wymaganiami KRI w Starostwie Powiatowym w Aleksandrowie Kujawskim i jednostkach organizacyjnych w 2026 roku

1. **Zakres i przedmiot zgodności z wymaganiami audytu KRI obejmuje przegląd systemów pod kątem zarządzania bezpieczeństwem informacji, umożliwiających realizację i egzekwowanie działań:**
   1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
   2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
   3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
   4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
   5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
   6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   g) zagrożenia bezpieczeństwa informacji,
   h) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   i) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   g) monitorowanie dostępu do informacji,
   h) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   i) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   q) dbałości o aktualizację oprogramowania,
   r) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   s) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   t) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   u) zapewnieniu bezpieczeństwa plików systemowych,
   v) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   w) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   x) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
15) rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

## 2.W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do:

1. dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, zgodnie z § 19 rozporządzeniem Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 773),
2. opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami. Dokumentacja poaudytowa (raport) ma być przygotowana zgodnie z zasadami dostępności cyfrowej dokumentów tekstowych opisanymi na stronie https://www.gov.pl/web/dostepnosc-cyfrowa/jak-zwiekszyc-dostepnosc-cyfrowa-dokumentow-tekstowych oraz oznaczona pełnokolorowym znakiem Funduszy Europejskich, znakiem barw RP i znakiem UE lub znakiem monochromatycznym (zgodnie z Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji).
3. realizacji przedmiotu zamówienia w siedzibie zamawiającego.

## 3.Szczegółowe parametry zamówienia:

1. **NAZWA JEDNOSTKI – Starostwo Powiatowe w Aleksandrowie Kujawskim, ul. Słowackiego 8, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 69
   b) Ilość budynków: 2
   c) Ilość serwerów fizycznych: 5
2. **NAZWA JEDNOSTKI – Zespół Szkół Nr 1 Centrum Kształcenia Praktycznego w Aleksandrowie Kujawskim, ul. Wyspiańskiego 4, 87-700 w Aleksandrów Kujawski**
   a) Ilość pracowników – 87 (w tym 67 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 0
3. **NAZWA JEDNOSTKI – Zespół Szkół Nr 2 im. Mjra H. Dobrzańskiego „Hubala" w Aleksandrowie Kujawskim, ul. Sikorskiego 2 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 79 ( w tym 69 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 1
4. **NAZWA JEDNOSTKI – Liceum Ogólnokształcące im. Stanisława Staszica w Ciechocinku, ul. Kopernika 1, 87-720 Ciechocinek**
   a) Ilość pracowników: 33 ( w tym 27 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 1
5. **NAZWA JEDNOSTKI – Szkoła Podstawowa Specjalna nr 4 im. Jana Pawła II w Aleksandrowie Kujawskim, ul. Strażacka 22, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 59 (w tym 48 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 0
6. **NAZWA JEDNOSTKI – Placówka Socjalizacyjna w Aleksandrowie Kujawskim, ul. Wyspiańskiego 4, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 15
   b) Ilość serwerów fizycznych: 1
7. **NAZWA JEDNOSTKI – Dom Pomocy Społecznej w Zakrzewie, ul. Inowrocławska 20, 87-707 Zakrzewo**
   a) Ilość pracowników: 79
   b) Ilość serwerów fizycznych: 1
8. **NAZWA JEDNOSTKI – Poradnia Psychologiczno - Pedagogiczna w Aleksandrowie Kujawskim, ul. Sikorskiego 3, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 18 ( w tym 13 pracowników pedagogicznych)
   b) Ilość serwerów fizycznych: 1
9. **NAZWA JEDNOSTKI – Powiatowe Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim, ul. Sikorskiego 3, 87-700 Aleksandrów Kujawski**
   a) Ilość pracowników: 13
   b) Ilość serwerów fizycznych: 1
10. **NAZWA JEDNOSTKI – Powiatowy Urząd Pracy w Aleksandrowie Kujawskim, ul. Przemysłowa 1, 87-700 Aleksandrów Kujawski**
    a) Ilość pracowników: 32
    b) Ilość serwerów fizycznych: 2
11. **NAZWA JEDNOSTKI – Zarząd Dróg Powiatowych w Aleksandrowie Kujawskim, Odolion ul. Szosa Ciechocińska 22, 87-700 Aleksandrów Kujawski**
    a) Ilość pracowników: 10
    b) Ilość serwerów fizycznych: 0