**Załącznik nr 5 do zapytania ofertowego**

**Projekt umowy nr …../2022**

zawarta w dniu ……………………..….2022 roku w ………………………………….…. pomiędzy:

**Gminą Ulhówek, ul. Kościelna 1/1; 22-678 Ulhówek, woj. lubelskie, NIP: 9211875007**

**zwaną w dalszej części umowy „Zamawiającym”, reprezentowanym przez:**

**Pana Łukasza Kłębka – Wójta Gminy**

**przy kontrasygnacie Z-ca Skarbnika Gminy Lucyny Ozdoba**

a

**………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………**

zwaną w dalszej części umowy „**Wykonawcą”** reprezentowanym przez:

**……………………………………………………………………………………………….**

**§1 Przedmiot umowy**

1. Przedmiotem niniejszej umowy jest przeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń w zakresie cyberbezpieczeństwa **zgodnie z założeniami programu Cyfrowa Gmina** z uwzględnieniem przedstawionej przez Wykonawcę oferty.
2. **Strony ustalają, że przedmiot umowy będzie wykonywany przy niezbędnej pomocy udzielonej przez Zamawiającego.**
3. Diagnoza cyberbezpieczeństwa musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa” stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina.
4. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
5. Prace stanowiące przedmiot zlecenia zostaną przeprowadzone z wykorzystaniem uznanych standardów międzynarodowych i dobrych praktyk w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, t.j.:

a) normy ISO (International Organization for Standardization);

b) ustawy o Krajowych Ramach Interoperacyjności.

1. Zamówienie jest współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

# **§ 2. Termin realizacji umowy**

1. Wykonawca zrealizuje przedmiot umowy nie później niż w ciągu **30 dni** od daty zawarcia umowy.
2. Za datę zawarcia umowy Zamawiający przyjmuje dzień, w którym zostanie ona podpisana przez obie Strony umowy.

**§ 3 Zobowiązania Wykonawcy**

1. Wykonawca zobowiązuje się do **wykonania audytu zgodnie z zakresem stanowiącym załącznik do niniejszej umowy.**
2. Wykonawca oświadcza, że umowa będzie wykonywana w siedzibie Zamawiającego, chyba że Zamawiający na wniosek Wykonawcy dopuści realizację umowy w całości lub w części za pomocą środków zdalnej komunikacji.
3. Wykonawca oświadcza, że posiada wszystkie wymagane uprawnienia do wykonywania przedmiotu umowy.
4. Wykonawca oświadcza, że dysponuje odpowiednią wiedzą oraz środkami technicznymi potrzebnymi do realizacji niniejszej umowy, w szczególności wykwalifikowanym personelem, sprzętem oraz oprogramowaniem.
5. W przypadku konieczności wykonania wizyt audytowych u dostawców usług teleinformatycznych Zamawiający powiadomi o tym swoich dostawców usług i ułatwi przeprowadzenie audytu.
6. Wykonawca s**porządzi i przekaże Zamawiającemu raport** z wykonanego audytu w terminie **14 dni roboczych** od dnia zakończenia sprawdzenia – raport zostanie przekazany w formie elektronicznej zaszyfrowanej.
7. Zamawiający może, nie później niż w terminie 7 dni roboczych po otrzymaniu raportu zgłosić Wykonawcy ewentualne zastrzeżenia co do raportu dotyczące kwestii merytorycznej, rozumianej jako niezgodność ze stanem faktycznym lub braków w jego treści.
8. Wykonawca zobowiązany jest odnieść się do zgłoszonych zastrzeżeń w terminie nie dłuższym niż 7 dni roboczych od dnia ich otrzymania.
9. Niezgłoszenie zastrzeżeń bądź przekroczenie ww. terminu równoznaczne jest z przyjęciem raportu w formie przedstawionej przez Wykonawcę.
10. Wykonawca wystawi dla osób wykonujących przedmiot umowy i uzyskujących dostęp do infrastruktury i/lub dokumentów Zamawiającemu upoważnienia do wykonywania takich czynności, w celu przedstawienia ich Zamawiającemu.
11. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w §3 ust. 1, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w ust. §3 ust. 1.
12. W przypadku, jeśli beneficjent projektu „Cyfrowa Gmina” tj. Centrum Projektów Polska Cyfrowa zmodyfikuje plik formularza, o którym mowa w powyższym ustępie, Wykonawca przekaże wynik diagnozy sporządzony w oparciu o aktualną wersję pliku. W dniu podpisania umowy plik formularza jest dostępny pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina, sekcja „Dokumentacja konkursowa” / ”Regulamin Konkursu”.

**§ 4 Zobowiązania Zamawiającego**

**Zamawiający** zobowiązuje się do:

1. Udostępnienia na żądanie Wykonawcy miejsca w swojej siedzibie niezbędnego do wykonywania niniejszej umowy.

2. Udzielania niezbędnych informacji i dokumentów (polityk i instrukcji dotyczących bezpieczeństwa w zakresie IT) w czasie wykonywania przedmiotu umowy:

1. wyrażenia zgody na dostęp Wykonawcy do infrastruktury informatycznej Zamawiającemu,
2. zapewnienia wolnych, stałych, co najmniej 2 adresów IP w każdej sieci lokalnej Zamawiającemu,
3. zapewnienia Wykonawcy kontaktu osobistego lub telefonicznego w niezbędnym zakresie z głównym informatykiem infrastruktury informatycznej Zamawiającemu, w czasie wykonywania testów,
4. udostępnienia Wykonawcy miejsca mającego na celu przetrzymywanie kopii zapasowych oraz danych zebranych podczas przeprowadzania testów,
5. stałego monitorowania łącza w sposób uzgodniony przez Strony w czasie wykonywania przez Wykonawcę prac audytowych,
6. wyznaczenia zespołu osób uprawnionych i przygotowanych merytorycznie do kontaktu ze Wykonawcą (w tym z Koordynatorem Audytu) w zakresie wykonania przedmiotu umowy poprzez przesłanie listy osób na adres: ………………………………… w terminie 7 dni od dnia podpisania umowy.

3. Szyfrowania przesyłanej drogą elektroniczną dokumentacji w sposób i narzędziami uzgodnionymi przez strony, w tym do udostępnienia własnego klucza publicznego PGP służącego do wymiany informacji.

**§ 5 Okres obowiązywania umowy**

Umowa zostaje zawarta na czas wykonania przedmiotu umowy.

**§ 6 Wynagrodzenie**

1. Za wykonanie przedmiotu umowy, określonego w §1 niniejszej umowy, Strony ustalają wynagrodzenie Zamawiający zobowiązuje się zapłacić Wykonawcy wynagrodzenie w wysokości …………………………… /słownie: …………………………… / PLN brutto zgodnie z ofertą Wykonawcy.

2. Wynagrodzenie płatne będzie przelewem bankowym na numer konta wskazany w fakturze w ciągu 14 dni od momentu otrzymania faktury, przy czym nie wcześniej niż po dokonaniu przez Zamawiającego odbioru raportu z przeprowadzonych testów lub niezgłoszenia zastrzeżeń w terminie określonym w § 3 ust. 7. Zamawiający upoważnia Wykonawcy do wystawienia faktury VAT bez jego podpisu oraz wyraża zgodę na przesłanie faktury VAT drogą elektroniczną w formie jawnej na adres e-mail: ………………………………………….. .

3. Za dzień zapłaty Strony ustalają dzień uznania rachunku bankowego Wykonawcy.

4. W przypadku uchybienia terminowi płatności Wykonawcy przysługują opłaty dodatkowe zgodne z obowiązującym prawem polskim i prawem unii europejskiej.

5. W przypadku nie otrzymania grantu przez gminę niniejsza umowa zostaje rozwiązana bez żadnych kosztów dla Zamawiającego.

**§ 7 Klauzula Poufności**

1. Strony postanawiają, że treść niniejszej umowy jest objęta tajemnicą w stosunku do osób trzecich i nie może być ujawniona przez Wykonawcę w czasie obowiązywania umowy i po jej ustaniu. To samo dotyczy wszelkich informacji uzyskanych przez Wykonawcę pośrednio lub bezpośrednio w związku z zawarciem lub realizacją niniejszej umowy.

2. Zamawiający wyraża zgodę na analizę danych na podstawie raportów z audytu i opracowań sumarycznych w celach statystycznych i marketingowych, uniemożliwiających jednoznaczne powiązanie zebranych danych z Zamawiającym.

3. Tajemnicę służbową Zamawiającego stanowi informacja dotycząca Zamawiającego o charakterze niejawnym, która nie jest znana lub nie powinna być znana publicznie, powzięta przez Wykonawcę w związku z wykonywaniem lub przy okazji wykonywania Umowy.

4. Za tajemnicę służbową, o której mowa w § 7 ust. 3 umowy uważa się w szczególności:

1. Rozkład pomieszczeń, ich przeznaczenie oraz zabezpieczenia i zasady ich ochrony,
2. Dane osobowe, w tym w szczególności dane pracowników i dane stron obsługiwanych przez Zamawiającego,
3. Rozwiązania techniczne i organizacyjne stosowane u Zamawiającego w celu zapewnienia bezpieczeństwa teleinformatycznego,
4. Wykryte w trakcie procesu kontroli słabości, luki systemów teleinformatycznych.

5. Wykonawca ma prawo do korzystania z informacji stanowiących tajemnicę Zamawiającego tylko w zakresie niezbędnym do realizacji niniejszej umowy.

6. Dokumenty powstałe w wyniku wykonywania przedmiotu umowy przechowywane są przez Wykonawcę w okresie 6 miesięcy od dnia zakończenia umowy.

7. Wykonawca oświadcza, że wszelkie informacje uzyskane w trakcie wykonywania przedmiotu umowy nie będą udostępniane osobom trzecim bez pisemnej zgody Zamawiającego.

8. Zamawiający zobowiązany jest do nieudostępniania osobom niebędącym stroną niniejszej umowy stosowanych przez Wykonawcę:

1. narzędzi kontroli;
2. procesów kontroli;
3. wszelkiej dokumentacji powstałej w wyniku działania Wykonawcy, w szczególności zaś raportu i dokumentów roboczych oraz dokumentów z kontroli;
4. powyższe zastrzeżenie obowiązuje wszystkich z wyłączeniem organów i podmiotów ustawowo uprawnionych do kontroli.

9. Wskazanie w niniejszej umowie imienia, nazwiska oraz danych kontaktowych osób równoznaczne jest z wyrażeniem przez Zamawiającego zgody na kontaktowanie się przez Wykonawcę ze wskazanymi osobami oraz uzyskiwanie i udzielanie informacji niezbędnych do wykonania niniejszej umowy.

10. Osobami do kontaktu ze strony Zamawiającego są:

……………. ……………………………………………………………… …………….

11. Osobami do kontaktu ze strony Wykonawcy są:

..................................................................................................

………………………………………………………………………………………………

12. Prawo do wykorzystywania wszystkich materiałów związanych z wykonywaniem przedmiotu umowy przysługuje jedynie Zamawiającemu i nie może być bez zgody Wykonawcy wykorzystywane przez jakiekolwiek inne podmioty, w tym podmioty kapitałowo lub osobowo powiązane z Zamawiającym z uwzględnieniem wyłączeń, o których mowa w pkt c) i d).

13. W związku z tym, iż dane do których dostęp może uzyskać Wykonawca w związku z wykonaniem Umowy mogą stanowić informacje objęte tajemnicą zawodową, Wykonawca zobowiązany jest stosować środki techniczne i organizacyjne zapewniające ochronę tych informacji, odpowiednio do istniejących zagrożeń. W szczególności środki te powinny zabezpieczyć informacje objęte tajemnicą zawodową przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, a także ich nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem. Wykonawca oświadcza, iż opracował i wdrożył procedury zapobiegające ujawnieniu i wykorzystaniu takich informacji. Zamawiający jest uprawniony do kontroli przestrzegania postanowień, o których mowa powyżej.

14. W przypadku gdy z wykonywaniem Umowy przez Wykonawcę będzie się wiązała konieczność dostępu do danych przetwarzanych przez Zamawiającego, osoby oddelegowane przez Wykonawcę do prac związanych z Umową, oświadczą że są zaznajomieni z treścią przepisów dotyczących tajemnicy zawodowej oraz zagadnień objętych RODO i Ustawą o ochronie danych osobowych, a także zagadnień wskazanych w przepisach wykonawczych do tej ustawy, oraz zobowiązują się przestrzegać tajemnicy zawodowej oraz zasad ochrony danych osobowych, obowiązujących u Zamawiającego, po zapoznaniu się z nimi przed rozpoczęciem prac oraz oświadczą że są świadomi odpowiedzialności wynikającej z naruszenia wymienionych zasad.

15. Zamawiający będzie administratorem danych osobowych przedstawicieli, pracowników i współpracowników Wykonawcy, przetwarzanych w związku z zawarciem i realizacją niniejszej umowy. Wykonawca zobowiązuje się przekazać informacje, o których mowa powyżej, wszystkim osobom, których dane udostępnił lub udostępni Zamawiający w związku z zawarciem i realizacją niniejszej umowy.

**§ 8 Usługi dodatkowe**

1. Zamawiający ma możliwość skorzystania z usług dodatkowych, wykraczających poza zakres przedmiotu umowy.

2. Zamawiający może zlecić wykonanie dodatkowej usługi pisemnie, poprzez złożenie przez uprawnioną osobę zamówienia na dedykowany e- mail: …………………………………………….. .

**§ 9 Postanowienia końcowe**

1. Niniejsza umowa podlega prawu Rzeczpospolitej Polskiej i będzie interpretowana zgodnie z przepisami tego prawa. W zakresie nieuregulowanym w niniejszej umowie zastosowanie mają przepisy Kodeksu cywilnego, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwane dalej „RODO” oraz ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych i ustawy z dnia 28 sierpnia 1997 o organizacji i funkcjonowaniu funduszy emerytalnych.

2. Wszelkie spory wynikające lub związane z wykonaniem niniejszej umowy, które nie zostaną rozwiązane przez Strony umowy na drodze polubownej, zostaną rozstrzygnięte przez sąd powszechny miejscowo właściwy.

3. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

4. Przedmiot umowy może być rozszerzony wg wzajemnych ustaleń i usankcjonowany aneksem do niniejszej umowy.

5. Niniejsza umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

………………………………………… ………………………………………….

*Data i podpis Zamawiającego* *Data i podpis Wykonawcy*

**Załączniki:**

1. Zakres audytu:
2. Audyt wykonujemy zgodnie z założeniami regulaminu projektu Cyfrowej Gminy.
3. Audyt jest zgodny z ustawą o KRI
4. Audyt przeprowadzamy w siedzibie gminy, przez dwóch audytorów w tym jeden; certyfikowany audytor wiodący ISO 27001 zgodnie z założeniami Regulaminu i rozporządzenia o kwalifikacjach audytorów drugi z certyfikatami konkretnych specjalizacji sieciowych i sprzętowych.
5. Przygotowywany jest raport wstępny. Raport wstępny obejmuje obserwacje i wskazówki do wdrożenia.
6. Raport końcowy (zlecony dodatkowo po wdrożeniu opisany w odrębnej umowie) wskazuje poprawnie wykonane prace i potwierdza bezpieczne wdrożenie.
7. Podatek VAT zgodnie z obowiązującymi stawkami w obowiązującym prawie.

Zakres prac objętych audytem:

|  |  |  |
| --- | --- | --- |
| L.p. | Opis wymagania | Podstawa |
| 1 | Wyznaczenie osoby do kontaktu | Art. 21 KSC |
| 2 | Przekazanie danych osoby wyznaczonej | Art. 22 pkt 5) KSC |
| 3 | Zapewnienie zarządzania incydentem | Art. 22 pkt 1) KSC |
| 4 | Zgłaszanie incydentu | Art. 22 pkt 2)  Art. 23 KSC |
| 5 | Zapewnienie obsługi incydentu | Art. 22 pkt 3) KSC |
| 6 | Zapewnienie dostępu do wiedzy | Art. 22 pkt 4) KSC |
| 7 | Opracowanie, ustanowienie i wdrożenie SZBI | Par. 20 KRI |
| 8 | Monitorowanie i przegląd SZBI | Par. 20 KRI |
| 9 | Doskonalenie SZBI | Par. 20 KRI |
| 10 | Aktualizowanie regulacji wewnętrznych | Par. 20 pkt 1) KRI |
| 11 | Inwentaryzacja sprzętu i oprogramowania | Par. 20 pkt 2) KRI |
| 12 | Przeprowadzanie okresowych analiz ryzyka | Par. 20 pkt 3) KRI |
| 13 | Postępowanie z ryzykiem | Par. 20 pkt 3) KRI |
| 14 | Zarządzanie uprawnieniami | Par. 20 pkt 4), 5) KRI |
| 15 | Szkolenia i uświadamianie | Par. 20 pkt 6) KRI |
| 16 | Monitorowanie dostępu do informacji | Par. 20 pkt 7) a), b) KRI |
| 17 | Monitorowanie nieautoryzowanych zmian | Par. 20 pkt 7) b) KRI |
| 18 | Zabezpieczenie nieautoryzowanego dostępu | Par. 20 pkt 7) c) KRI |
| 19 | Ustanowienie zasad bezpiecznej pracy mobilnej | Par. 20 pkt 8) KRI |
| 20 | Zabezpieczenie informacji przed nieuprawnionym ujawnieniem | Par. 20 pkt 9) KRI |
| 21 | Zabezpieczenie informacji przed nieuprawnioną modyfikacją | Par. 20 pkt 9) KRI |
| 22 | Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem | Par. 20 pkt 9) KRI |
| 23 | Zawieranie w umowach serwisowych zapisów o bezpieczeństwie | Par. 20 pkt 10) KRI |
| 24 | Ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania | Par. 20 pkt 11) KRI |
| 25 | Aktualizowanie oprogramowania | Par. 20 pkt 12) a) KRI |
| 26 | Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu | Par. 20 pkt 12) b) KRI |
| 27 | Ochrona systemu przed błędami | Par. 20 pkt 12) c) KRI |
| 28 | Stosowanie mechanizmów kryptograficznych w systemach | Par. 20 pkt 12) d) KRI |
| 29 | Zapewnienie bezpieczeństwa plików systemowych | Par. 20 pkt 12) e) KRI |
| 30 | Zarządzanie podatnościami systemów | Par. 20 pkt 12) f), g) KRI |
| 31 | Kontrola zgodności systemów z regulacjami | Par. 20 pkt 12) h) KRI |
| 32 | Zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok | Par. 20 pkt 14) KRI |

|  |  |
| --- | --- |
| l.p. | **Zagadnienie** |
| **1** | **Dokumentacja potwierdzająca wykonane działania wskazanego w ustawie** |
| 1.1 | Czy zostały zidentyfikowane usługi publiczne, których świadczenie zależy od bezpieczeństwa systemów informatycznych? |
| 1.2 | Czy zostały wskazane osoby (podmioty) odpowiedzialne za zarządzanie incydentami? |
| 1.3 | Czy podmiot publiczny realizuje zadania publikowania informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa oraz możliwych, skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, tj. zadań zawartych w art. 22 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz. 1560)? |
| 1.4 | Czy została wyznaczona i zgłoszona do właściwego CSIRT, osoba kontaktowa, o której mowa w art. 21 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz. 1560)? |
| **2** | **Opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne** |
| 2.1 | Czy wszystkie elementy składowe systemu informatycznego zostały zinwentaryzowane? |
| 2.2 | Czy dla każdego systemu informatycznego utrzymywana jest aktualna lista osób odpowiedzialnych za jego bezpieczną eksploatację? |
| **3** | **Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne** |
| 3.1 | Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne? |
| 3.2 | Czy dostępne są potwierdzenia działań wynikających z komunikacji z procesem szacowania ryzyka SI\_OUK? |
| 3.3 | Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń? |
| 3.4 | Czy istnieje dokumentacja architektury sieci? |
| 3.5 | Czy istnieje baza danych konfiguracji urządzeń aktywnych? |
| 3.6 | Czy istnieje dokumentacja zmian w systemach informacyjnych? |
| 3.7 | Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym? |
| 3.8 | Czy są dostępne umowy z dostawcami (wsparcie techniczne)? |
| 3.9 | Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego? |
| 3.10 | Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego? |
| 3.11 | Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych? |
| 3.12 | Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego? |
| **4** | **Dokumentacja procesu zarządzania incydentami** |
| 4.1 | Czy wdrożone jest monitorowanie i wykrywanie incydentów? Kto za nie odpowiada? |
| 4.2 | Czy istnieje procedura informowania o wykrytych incydentach? |
| 4.3 | Czy istnieją procedury reagowania na incydenty? |
| **5** | **Aspekty techniczne do weryfikacji** |
| 5.1 | Wyniki audytu serwisów WWW z uwzględnieniem:  - wersji serwera HTTP  - wersji systemu CMS (o ile występuje)  - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.)  - dostępność kompetentnego personelu do utrzymania serwisów |
| 5.2 | Wyniki audytu serwisów pocztowych z uwzględnieniem:  - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC  - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS  - dostępności kompetentnego personelu do utrzymania serwisów |
| 5.3 | Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem:  - stosowania mechanizmów segmentacji sieci  - izolacji urządzeń końcowych użytkowników  - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji  - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa  - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej |
| 5.4 | Wyniki audytu połączenia z siecią Internet z uwzględnieniem:  - monitorowania ruchu wchodzącego i wychodzącego  - stosowanych zabezpieczeń przed atakami DDoS  - stosowanych zabezpieczeń przed wyciekiem informacji (DLP)  - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.)  - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet |