**Załącznik nr 1 do Ogłoszenia**

**Załącznik do Umowy**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA - PLAN AUDYTU**

**Audyt dokumentacji i procesów**

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)
2. wyznaczenie osoby do kontaktu – Art. 21 KSC;
3. przekazanie danych osoby wyznaczonej – Art. 22 pkt 5) KSC;
4. zapewnienie zarządzania incydentem – Art. 22 pkt 1) KSC;
5. zgłaszanie incydentu – Art. 22 pkt 2) Art. 23 KSC;
6. zapewnienie obsługi incydentu – Art. 22 pkt 3) KSC;
7. zapewnienie dostępu do wiedzy – Art. 22 pkt 4) KSC;
8. opracowanie, ustanowienie i wdrożenie SZBI – Par. 20 KRI;
9. monitorowanie i przegląd SZBI – Par. 20 KRI;
10. doskonalenie SZBI – Par. 20 KRI;
11. aktualizowanie regulacji wewnętrznych – Par. 20 pkt 1) KRI;
12. inwentaryzacja sprzętu i oprogramowania – Par. 20 pkt 2) KRI;
13. przeprowadzanie okresowych analiz ryzyka – Par. 20 pkt 3) KRI;
14. postępowanie z ryzykiem – Par. 20 pkt 3) KRI;
15. zarządzanie uprawnieniami – Par. 20 pkt 4), 5) KRI;
16. szkolenia i uświadamianie – Par. 20 pkt 6) KRI;
17. monitorowanie dostępu do informacji – Par. 20 pkt 7) a), b) KRI;
18. monitorowanie nieautoryzowanych zmian – Par. 20 pkt 7) b) KRI;
19. zabezpieczenie nieautoryzowanego dostępu – Par. 20 pkt 7) c) KRI;
20. ustanowienie zasad bezpiecznej pracy mobilnej – Par. 20 pkt 8) KRI;
21. zabezpieczenie informacji przed nieuprawnionym ujawnieniem – Par. 20 pkt 9) KRI;
22. zabezpieczenie informacji przed nieuprawnioną modyfikacją – Par. 20 pkt 9) KRI;
23. zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – Par. 20 pkt 9) KRI;
24. zawieranie w umowach serwisowych zapisów o bezpieczeństwie – Par. 20 pkt 10) KRI;
25. ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – Par. 20 pkt 11) KRI;
26. aktualizowanie oprogramowania – Par. 20 pkt 12) a) KRI;
27. minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – Par. 20 pkt 12) b) KRI;
28. ochrona systemu przed błędami – Par. 20 pkt 12) c) KRI;
29. stosowanie mechanizmów kryptograficznych w systemach – Par. 20 pkt 12) d) KRI;
30. zapewnienie bezpieczeństwa plików systemowych – Par. 20 pkt 12) e) KRI;
31. zarządzanie podatnościami systemów – Par. 20 pkt 12) f), g) KRI;
32. kontrola zgodności systemów z regulacjami – Par. 20 pkt 12) h) KRI;
33. zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – Par. 20 pkt 14) KRI.
34. Ocena wybranych aspektów bezpieczeństwa systemów informatycznych
35. dokumentacja potwierdzająca wykonane działania wskazanego w ustawie;
36. opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne;
37. dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne;
38. dokumentacja procesu zarządzania incydentami;
39. aspekty techniczne do weryfikacji.
40. Ocena dojrzałości wybranych procesów bezpieczeństwa
41. ochrona przed kodem szkodliwym;
42. ochrona sieci i połączeń;
43. ochrona urządzeń końcowych;
44. zarządzanie tożsamością i autoryzacją dostępu;
45. ochrona fizyczna systemów IT;
46. bezpieczeństwo urządzeń drukujących;
47. zarządzanie podatnościami;

4. Opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny.

**Testy penetracyjne infrastruktury sieciowej**

1. Przedstawienie założeń Audytu

Audyt wykonywany będzie w sposób manualny oraz automatyczny za pomocą specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy i doświadczeń. Testy zostaną przeprowadzone w oparciu o OSSTMM (Open Source Security Testing Methodology Manual).

1. Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci.
2. Skanowanie sieci – rekonesans sieci
3. Sprawdzenie jakie hosty są w sieci widoczne, ile ich jest, usługi jakie są uruchomione na hostach, jakie systemy operacyjne działają na wykrytych hostach. W szczególności ten etap polega na:
4. skanowaniu sieci w poszukiwaniu wszystkich podłączonych hostów;
5. wykryciu czy jest dostęp do innych podsieci z danej podsieci;
6. wykryciu usług działających na hostach podłączonych do sieci;
7. wykryciu podatności na wybranych hostach w sieci.
8. Skanowanie będzie powtórzone dla każdej wskazanej przez zamawiającego sieci

Przeprowadzenie skanowania w prawidłowo działającej sieci nie powinno mieć negatywnego wpływu na działanie sieci. Po przeskanowaniu sieci wraz z Zamawiającym zostanie wybrana pula hostów do dalszego badania.

1. Skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), które zostały wybrane na podstawie wcześniejszej analizy
2. weryfikacja występowania luk bezpieczeństwa dla konkretnych usług w zależności od wykrytej usługi;
3. weryfikacja haseł;
4. weryfikacja dostępu użytkowników do odpowiednich usług;
5. weryfikacja możliwości dostępu do usługi;
6. weryfikacja luk bezpieczeństwa w systemie operacyjnym;
7. weryfikacja luk bezpieczeństwa w oprogramowaniu firm trzecich.
8. Sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy - weryfikacja haseł w usługach umożliwiających logowanie.
9. Sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł.
10. Weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych.
11. Weryfikacja zabezpieczeń urządzeń sieciowych
12. badanie odporności switchy na ataki sieciowe;
13. weryfikacja zabezpieczeń monitoringu wizyjnego.
14. Testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej
15. weryfikacja pod kątem dostępu;
16. weryfikacja pod kątem zabezpieczeń;
17. wykrycie możliwości przechwycenia haseł;
18. w przypadku przechwycenia hasła – weryfikacja pod katem możliwości złamania hasła.
19. Zdalne testy adresów publicznych – 8 adresów.
20. Badanie ankietowe;
21. Badanie ankietowe pracowników działu IT oraz pracowników Zamawiającego z wiedzy o bezpieczeństwie sieci i procedurach IT stosowanych przez Zamawiającego. Grupa ankietowanych pracowników zostanie ustalona podczas Audytu.
22. Testy socjotechniczne
23. kontakt telefoniczny – do 5 osób;
24. kampanie phishingowe dla całgo urzędu.
25. Wykonanie raportu zawierającego
26. opis wszystkich elementów, które zostały poddane audytowi;
27. podział podatności ze względu na ryzyko:
    * wysoki
    * średni
    * niski
28. wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności.
29. wylistowanie wszystkich podatności ze względu na ryzyko:

* wysoki
* średni
* niski

1. określenie bezpieczeństwa informatycznego w urzędzie poprzez wskazanie ilości i rodzaju znalezionych podatności.