Znak sprawy WRiZP.272.1.1.2025 **Załącznik nr 1 do SWZ**

OPIS PRZEDMIOTU ZAMÓWIENIA

Zadanie I: Przeprowadzenie dwóch audytów zgodności z Krajowymi Ramami Interoperacyjności dla Starostwa Powiatowego oraz 13 jednostek organizacyjnych

I. Zakres audytu KRI:

1. Wizja lokalna + skanowanie infrastruktury **– w siedzibie Zamawiającego i 13 jednostkach organizacyjnych oraz zdalnie obejmująca:**
   a) wizję lokalną miejsc kluczowych dla działania infrastruktury,
   b) ocenę bezpieczeństwa pomieszczenia serwerowego, w tym kontroli dostępu, monitoringu i klimatyzacji,
   c) występowanie pojedynczych punktów awarii,
   d) weryfikację, czy sprzęt jest chroniony przed nieuprawnionym dostępem oraz czynnikami środowiskowymi,
   e) wywiad techniczny,
   f) skanowanie wewnętrznej infrastruktury. Próba określenia podatności na zagrożenia w związku z występowaniem potencjalnych luk w zabezpieczeniach w systemach operacyjnych i usługach sieciowych.
2. Bezpieczeństwo danych. Sprawdzenie dobrych praktyk dotyczących wykonywania kopii zapasowych. Przegląd polityk tworzenia kopii.
3. Audyt według wymogów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. 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) w zakresie bezpieczeństwa informacji.
4. Raport z audytu winien być podpisany przez audytora dokonującego audytu i dostarczony do Zamawiającego.
5. Audyt winien być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzeniu audytu, o którym mowa w rozporządzeniu Ministra Cyfryzacji z 12

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. poz. 1999).

6. Audyt winien być przeprowadzony w zakresie spełniającym wymagania określone w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd", opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem http://www.gov.pl/cppc/cyberbezpieczny-samorzad.
7. Raport wraz z podsumowaniem powinien zostać omówiony na spotkaniu z najwyższym kierownictwem urzędu, zespołem informatyków, Inspektorem Ochrony Danych i innymi osobami wskazanymi przez Zamawiającego. Wyniki raportu powinny wskazywać możliwości rozwiązania odkrytych defektów i nakreślić plan działań naprawczych.
8. Wykonawca przekaże raport z przeprowadzonego audytu w postaci pliku wypełnionego arkusza kalkulacyjnego formularza (osobny dla każdej jednostki), tj. Formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiącego załącznik nr 6 do Regulaminu Konkursu Grantowego, podpisanego podpisem cyfrowym (kwalifikowanym podpisem elektronicznym/podpisem zaufanym/podpisem osobistym) przez osobę posiadającą odpowiednie uprawnienia wykazane w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu oraz w postaci dwóch wydrukowanych i podpisanych egzemplarzy przedmiotowego formularza wraz ze szczegółowym podsumowaniem.
9. Prawa autorskie majątkowe w odniesieniu do wszystkich dokumentów będących utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskich i prawach pokrewnych (Dz.U. z 2025 r., poz. 24 z póź. zm.) zwanych dalej „utworami", dostarczonych przez Wykonawcę w trakcie realizacji przedmiotu zamówienia przechodzą na Zamawiającego z chwilą ich dostarczenia Zamawiającemu. Z tą też chwilą na Zamawiającego przechodzi prawo własności do nośników, na których utwory zostały utrwalone. Szczegóły w tym zakresie zostaną uregulowane w umowie dotyczącej realizacji przedmiotu zamówienia.
10. Harmonogram poszczególnych audytów:
    - Audyt KRI nr 1 – do 31.05.2025 roku,
    - Audyt KRI nr 2 – do 31.10.2025 roku,

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

Zadanie II - Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji wraz z aktualizacją i audytem zgodności dla Starostwa Powiatowego oraz 13 jednostek organizacyjnych

Zakres audytu SZBI:

1. Przegląd obejmie następujące obszary:
    a) obszar dot. kwestii organizacyjnych
    b) obszar dot. kwestii prawnych
    c) obszar dot. kwestii informatycznych
    d) obszar dot. kwestii zasobów ludzkich
    e) obszar dot. kwestii bezpieczeństwa fizycznego
2. Wizja lokalna + skanowanie infrastruktury **– w siedzibie Zamawiającego i 13 jednostkach organizacyjnych oraz zdalnie obejmująca:**
    a) wizję lokalną miejsc kluczowych dla działania infrastruktury,
    b) ocenę bezpieczeństwa pomieszczenia serwerowego, w tym kontroli dostępu, monitoringu i klimatyzacji,
    c) występowanie pojedynczych punktów awarii,
    d) weryfikację, czy sprzęt jest chroniony przed nieuprawnionym dostępem oraz czynnikami środowiskowymi,
    e) wywiad techniczny,
    f) skanowanie wewnętrznej infrastruktury. Próba określenia podatności na zagrożenia w wykrytych systemach operacyjnych i usługach sieciowych.
3. Ocena bezpieczeństwa organizacji z sieci internet – skanowanie z zewnątrz. Ocena urządzeń brzegowych pod kątem: podstawowej konfiguracji, wersji zainstalowanego systemu operacyjnego i możliwych ścieżek aktualizacji, polityk bezpieczeństwa na urządzeniu UTM, podziału sieci fizycznej na sieci logiczne z uwzględnieniem segmentacji sieci oraz izolacji systemów kluczowych.
4. Bezpieczeństwo danych. Sprawdzenie dobrych praktyk dotyczących wykonywania kopii zapasowych. Przegląd polityk tworzenia kopii.
5. Raport z audytu winien być podpisany przez audytora dokonującego audyt i dostarczony do Zamawiającego.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

OPRACOWANIE I WDROŻENIE SZBI

1. Wykonawca, na podstawie wyników Audytu KRI oraz Audytu Zgodności SZBI opracuje dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI) dostosowanego do potrzeb Zamawiającego.
2. SZBI, który opracuje Wykonawca, będzie stanowił system zarządzania bezpieczeństwem informacji, o którym mowa w § 19 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773) bądź w zastępujących go, odpowiednich przepisach wykonawczych do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 z póź. zm.).
3. SZBI powinien być zgodny z rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773) i spełniać wymagania normy PN-ISO/IEC 27001, w tym obejmować czternaście następujących obszarów mających wpływ na bezpieczeństwo w organizacji Zamawiającego:
    1) Polityka Bezpieczeństwa;
    2) organizacja bezpieczeństwa informacji;
    3) bezpieczeństwo zasobów ludzkich;
    4) zarządzanie aktywami;
    5) kontrola dostępu;
    6) kryptografia;
    7) bezpieczeństwo fizyczne i środowiskowe;
    8) bezpieczna eksploatacja;
    9) bezpieczna komunikacja;
    10) pozyskiwanie, rozwój i utrzymanie systemów;
    11) relacje z dostawcami;
    12) zarządzanie incydentami związanymi z bezpieczeństwem informacji;
    13) aspekty bezpieczeństwa w zarządzaniu ciągłością działania;
    14) zgodność z wymaganiami prawnymi i własnymi standardami.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

Ponadto SZBI powinien uwzględniać wymagania norm: PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762. 4. SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:

1) rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773);
2) 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1);
3) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
4) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 z późn. zm.);
5) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902);
6) ustawy z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowiska (Dz. U. z 2024 r. poz. 1112 z późn. zm.);
7) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 z późn. zm.);
8) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 z późn. zm.);

oraz uwzględniać wewnętrzne akty prawne obowiązujące u Zamawiającego.

4. W ramach opracowania SZBI Wykonawca między innymi:
   1) zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią Sprawozdania zaakceptowanego przez Zamawiającego;
   2) uwzględni w szczególności następujące zagadnienia:
      a) określenie organizacji bezpieczeństwa informacji,

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

b) identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
c) szacowanie ryzyka oraz postępowanie z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
d) bezpieczeństwo w procesach zarządzania zasobami ludzkimi,
e) szkolenia z zakresu bezpieczeństwa informacji,
f) kontrola dostępu,
g) bezpieczeństwo fizyczne i środowiskowe,
h) klasyfikacja informacji,
i) odpowiedzialność za zasoby,
j) postępowanie z nośnikami informacji,
k) użytkowanie urządzeń mobilnych i praca zdalna,
l) zarządzanie sprzętem informatycznym,
m) instalacja oprogramowania,
n) ochrona przed oprogramowaniem złośliwym,
o) kopie zapasowe,
p) zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
q) zarządzanie dokumentacją infrastruktury informatycznej,
r) monitorowanie systemów informatycznych,
s) zarządzanie pojemnością,
t) serwis i konserwacja infrastruktury informatycznej,
u) zarządzanie podatnościami technicznymi,
v) zarządzanie incydentami bezpieczeństwa,
w) zabezpieczenia kryptograficzne,
x) bezpieczeństwo sieci i transmisji danych,
y) ochrona własności intelektualnej,
z) bezpieczeństwo informacji w relacjach z dostawcami,
aa) ciągłość działania,
bb) zasady bezpieczństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
cc) weryfikacja zgodności z wymaganiami prawnymi,

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

dd) korzystanie z poczty elektronicznej i Internetu,

ee) zarządzanie usługami informatycznymi,

ff) utrzymanie i doskonalenie SZBI,

gg) przeprowadzanie audytów SZBI.

5. Wykonawca wraz z SZBI przedstawi zestawienie, zwane „Zestawieniem", w którym wykaże spełnienie przez SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, w tym rozporządzenia KRI, a także odpowiednich norm.
6. SZBI oraz Zestawienie zostaną przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie pisemnej.
7. Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę SZBI, w tym do rodzaju dokumentów, ich liczby, nazewnictwa, zakresu merytorycznego. Uwagi Zamawiającego powinny być każdorazowo uwzględnione przez Wykonawcę. W przypadku, gdyby proponowane przez Zamawiającego zmiany mogły powodować niezgodność dokumentacji z umową, Wykonawca poinformuje o tym wcześniej Zamawiającego, uzasadniając swoje stanowisko – w takim przypadku Zamawiający podejmie ostateczną decyzję w zakresie konieczności uwzględnienia jego uwag przez Wykonawcę.
8. Aktualizacja dokumentacji SZBI – po wykonaniu drugiego audytu zgodności KRI (termin drugiego audytu KRI u Zamawiającego – do 31.10.2025 r.).
9. Harmonogram poszczególnych części zadania:
   - Audyt SZBI – do 31.05.2025 roku,
   - Opracowanie i wdrożenie SZBI – do 31.10.2025 roku,
   - Aktualizacja SZBI – do 30.11.2025 roku.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

<u>Zadanie III - Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa oraz socjotechniki dla Starostwa Powiatowego oraz 13 jednostek organizacyjnych – 186 osób</u>

Głównym tematem stacjonarnego szkolenia ma być omówienie poprawnych zasad związanych z cyberbezpieczeństwem i socjotechniki oraz uzyskanie szczegółowych informacji związanych z zagrożeniami w sieci, takimi jak: phishing, ransomware oraz malware. Na szkoleniu muszą zostać poruszone również sposoby przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami. Zakres szkolenia powinien uwzględniać wyniki raportu z przeprowadzonego pierwszego audytu KRI oraz audytu SZBI. Wykonawca winien posiadać stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. Zamawiający nie dopuszcza przeprowadzenia szkoleń w sposób zdalny. Wszystkie szkolenia muszą się odbyć w siedzibie Zamawiającego – stacjonarnie. Szkolenie winno być przeprowadzone w taki sposób, by przekazywana wiedza była zrozumiała dla każdego, niezależnie od stopnia zaawansowania technicznego. Forma szkolenia powinna być lekka i przyjemna. Szkolenie powinno nauczyć pracowników jak wykrywać i poprawnie reagować na skierowane bezpośrednio w nich, jak i w całą instytucję ataki. Wykonawca przeszkoli pracowników w 6 grupach szkoleniowych po 31 osób. Czas przeznaczony na szkolenie jednej grupy nie może być krótszy niż 1,5 godziny. Wykonawca uzgodni harmonogram szkoleń z przedstawicielem Zamawiającego. Szkolenia będą odbywać się w dni robocze w godzinach pracy Zamawiającego.

1) Minimalny/ramowy zakres szkolenia:
   - główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika,
   - polityka bezpieczeństwa w organizacji,
   - definicja incydentu bezpieczeństwa i zasady postępowania z incydentem,
   - bezpieczeństwo fizyczne,
   - rodzaje ataków, w tym m.in. phishing, ransomware oraz malware i sposoby przeciwdziałania oraz zabezpieczania się przed tymi zagrożeniami,
   - prawidłowe korzystanie z oprogramowania antywirusowego, zabezpieczenie informatycznych nośników danych,
   - zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia,
   - przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych,

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

- szyfrowanie dokumentów i poczty elektronicznej,
- polityka haseł,
- zarządzanie dostępem i tożsamością.

2) W ramach organizacji szkoleń Zamawiający zapewni:
   - rekrutację osób biorących udział w szkoleniach,
   - salę szkoleniową zapewniającą warunki do przeprowadzenia szkolenia, wyposażoną w projektor multimedialny,
   - dostęp do sieci Internet.
3) W ramach organizacji szkoleń Wykonawca zapewni:
   - kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń,
   - mobilny sprzęt komputerowy z licencjami oprogramowania i pozostałymi akcesoriami niezbędnymi do przeprowadzenia szkolenia,
   - certyfikat, dyplom itp. dokument dla uczestników szkolenia poświadczający ukończenie szkolenia.
4) Harmonogram zadania:
   - Szkolenia w okresie od 01.05.2025 roku do 31.10.2025 roku.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23

<u>Zadanie IV – Organizacja specjalistycznego szkolenia ESET Client & Network Administrator dla 5 osób</u>

Specjalistyczne szkolenie ESET Client & Network Administrator obejmuje:

1. Szkolenie z zakresu oprogramowania antywirusowego i zabezpieczającego marki ESET oraz konsoli zarządzającej ESET PROTECT posiadanego przez Zamawiającego dla pięciu osób wskazanych przez Zamawiającego.
2. Szkolenie w formie zdalnej zakończone egzaminem oraz wydawanym na jego podstawie certyfikatem „ESET Managed Client Security Professional" autoryzowanym przez firmę ESET.
3. Szkolenie winno odbyć się w terminie od maja 2025 roku do października 2025 roku. Możliwe jest dołączenie do grupy uczestników w terminie planowanym przez Wykonawcę. Wykonawca winien zarezerwować w wybranym terminie miejsca dla pięciu osób oraz powiadomić te osoby o terminie szkolenia z co najmniej 2 tygodniowym wyprzedzeniem.
4. Przewidywany czas potrzebny na odbycie szkolenia oraz egzaminu nie więcej niż 3 dni robocze (24 godziny robocze) ogółem.
5. Szkolenie powinno obejmować co najmniej poniższy zakres:
   5.1. Różnice między ESET PROTECT On-Prem oraz ESET PROTECT
   5.2. Różnice między ESET Endpoint Antivirus i ESET Endpoint Security
   5.3. Wyjaśnienie platformy ESET Business Account i zasad licencjonowania oraz ćwiczenia z tego zakresu
   5.4. Instalacja i aktualizacja rozwiązania ESET PROTECT On-Prem oraz ćwiczenia z tego zakresu
   5.5. Zarządzanie kontami administratorów i uprawnieniami oraz ćwiczenia z tego zakresu
   5.6. Zdalna instalacja i omówienie ESET Management Agent oraz ćwiczenia z tego zakresu
   5.7. Wyjaśnienie grup statycznych i dynamicznych oraz różnic pomiędzy nimi
   5.8. Wyjaśnienie zadań klienta, zadań serwera oraz wyzwalaczy
   5.9. Sposoby zdalnej instalacji klienta ESET
   5.10. Omówienie najczęściej spotykanych scenariuszy wdrożeń
   5.11. Omówienie funkcji ESET Endpoint Security
   5.12. Ochrona antywirusowa
   5.13. Zarządzanie aktualizacjami
   5.14. Wyjaśnienie polityk ustawień i ich dziedziczenie oraz ćwiczenia z tego zakresu
   5.15. Omówienie rozwiązania ESET Bridge

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

5.16. Omówienie zapory osobistej oraz ćwiczenia z tego zakresu
5.17. Typowe scenariusze wdrożeń oraz ćwiczenia z tego zakresu
5.18. Omówienie modułu antyspam
5.19. Omówienie systemu powiadomień
5.20. Omówienie systemu raportowania
5.21. Omówienie modułu kontroli do stron internetowych oraz ćwiczenia z tego zakresu
5.22. Omówienie modułu kontroli dostępu do urządzeń oraz ćwiczenia z tego zakresu
5.23. Migracja z rozwiązania ESET PROTECT On-Prem do ESET PROTECT oraz ćwiczenia z tego zakresu
5.24. Wdrożenie ESET Endpoint Security for Android oraz ćwiczenia z tego zakresu
5.25. Rozwiązywanie typowych problemów

6. Harmonogram zadania:
   - Szkolenie w okresie od 01.05.2025 roku do 31.10.2025 roku

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23