1. Przedmiotem zamówienia jest:

**Część I** - przeprowadzenie diagnozy cyberbezpieczeństwa, w Urzędzie Gminy Suchy Las, w tym opracowanie raportu zawierającego wnioski i rekomendacje przeprowadzenie szkolenia w zakresie cyfrowego bezpieczeństwa wewnętrznego informacji w Urzędzie gminy Suchy Las,

1.1. **Diagnoza cyberbezpieczeństwa** – szczegółowy opis przedmiotu zamówienia – załącznik nr 1.

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji oraz opracowania dokumentacji poaudytowej – raport z wytycznymi do doskonalenia i rekomendacjami.

1) Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 ze zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 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 2017 r. poz. 2247, ze zm.).

2) Diagnoza cyberbezpieczeństwa musi zostać wykonana zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronie internetowej Centrum Projektów Polska Cyfrowa https://www.gov.pl/web/cppc/cyfrowa-gmina - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa – załącznik nr 8.

3) Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. 1.2. **Szkolenie z cyfrowego bezpieczeństwa** – szczegółowy opis przedmiotu zamówienia – załącznik nr 1.

1. Szkolenie poaudytowe pracowników Urzędu z zakresu:

- bezpieczeństwa pracy w systemach informatycznych, ochrony danych osobowych, legalności oprogramowania w oparciu o uzyskane wyniki audytu i testów, przedstawienie zaleceń,

- przeprowadzenie testów penetracyjnych (przeprowadzenie kontrolowanego „ataku” na system teleinformatyczny mający na celu praktyczną ocenę bieżącego stanu bezpieczeństwa tego systemu, w szczególności obecności znanych podatności i odporności na próby przełamania zabezpieczeń),

- przeprowadzenie testów socjotechnicznych (polegajacych na próbach uzyskania nieautoryzowanego dostępu do danych poprzez „atakowanie” pracowników - phishing, telefony itp. – w kontrolowany sposób).

2. Rekomendowana forma przeprowadzenia szkolenia: stacjonarna/on-line.