**Załącznik 6D do SWZ**

**W związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego w trybie podstawowym pn.**:

**„Rozbudowa, modernizacja i szkolenia w ramach realizacji projektu Cyfrowa Gmina realizowanego w czterech zadaniach”** (nr postępowania BI.271.23.2023) poniżej przedstawiamy specyfikację techniczną dla:

**Zadania nr 4:** Szkolenie z zakresu cyberbezpieczeństwa.

* 1. **Szkolenie z cyberbezpieczeństwa**

Forma szkolenia: online oraz jedno spotkanie kontaktowe.

Szkolenia online powinny być nagrywane i przekazane Zamawiającym jako materiał dydaktyczny.

W ten czas dla uczestników nie mogących uczestniczyć w szkoleniu powinna być udostępniona możliwość odtwarzanie filmów szkoleniowych.

Cykl szkoleń (online) powinien zawierać min. 5 lekcji o czasie nie krótszym niż 45 minut każde.

Okres udostępnienia szkolenia dla uczestników min. 6 miesięcy.

* 1. Zakres szkolenia teoretycznego (onilne) i jego tematyka:

1. Identyfikacja i istota cyberbezpieczeństwa,

Istota cyberbezpieczeństwa polega na opracowaniu i wdrożeniu odpowiednich strategii, procedur i narzędzi mających na celu ochronę systemów komputerowych i sieci przed zagrożeniami. Cyberbezpieczeństwo obejmuje różne obszary ochrony, takie jak:

1. **Ochrona sieci**
2. **Ochrona danych**
3. **Ochrona systemów**
4. **Świadomość i szkolenia**
5. **Zarządzanie ryzykiem**

Istota cyberbezpieczeństwa polega na ciągłym monitorowaniu, analizie i aktualizacji środków bezpieczeństwa

1. Podstawowe pojęć związanych z cyberbezpieczeństwem, np.: https, IP, TCP, domena, ASE-256, komunikator i inne.

Omówienie podstawowych pojęć związanych z cyberbezpieczeństwem:

1. **HTTPS (Hypertext Transfer Protocol Secure)**
2. **IP (Internet Protocol)**
3. **TCP (Transmission Control Protocol)**
4. **Domena**
5. **AES-256 (Advanced Encryption Standard)**
6. **Komunikator**

W cyberbezpieczeństwie zrozumienie tych pojęć jest ważne, ponieważ są one często wykorzystywane w kontekście zabezpieczeń sieciowych, szyfrowania danych i bezpiecznej komunikacji w sieci. Warto również pamiętać, że dziedzina cyberbezpieczeństwa jest dynamiczna, a nowe pojęcia i technologie mogą pojawiać się w miarę rozwoju technologii i zmian w zagrożeniach.

1. Zasady funkcjonowania i rozpoznawanie zagrożeń typu: phishing i ransomware.

Zasady funkcjonowania i rozpoznawanie zagrożeń typu phishing i ransomware są niezwykle istotne w dziedzinie cyberbezpieczeństwa. Należy omówić zasady i podać wskazówki, które pomogą zrozumieć te zagrożenia i chronić się przed nimi:

1. Phishing:
2. Ransomware:
3. Zasady bezpiecznego korzystania z poczty elektronicznej;

Korzystanie z poczty elektronicznej jest powszechne, dlatego istotne jest zapoznanie się z zasadami bezpiecznego jej użytkowania.

Należy omówić podstawowe zasady:

1. Tworzenie haseł
2. Zagrożenia phishingowe
3. Zaufane źródła
4. Załączniki od nieznanych źródeł
5. Bezpieczne połączenie
6. Aktualizacje oprogramowania
7. SPAM
8. Sposoby logowania się
9. Bezpieczeństwo podczas korzystania z przeglądarek internetowych: Mozilla Firefox, Google Chrome, Microsoft Edge, Apple Safari. Jak bezpiecznie komunikować się w Internecie, należy omówić zasady dotyczących bezpieczeństwa w kontekście poszczególnych przeglądarek:

* **Mozilla Firefox:**
* **Google Chrome:**
* **Microsoft Edge:**
* **Apple Safari:**

1. Prywatność w sieci, czyli: trakery, ciastka i tryb incognito

Ochrona prywatności w sieci jest ważnym aspektem bezpiecznego korzystania z internetu. Kilka pojęć związanych z prywatnością online to trakery, ciastka (cookies) i tryb incognito.

1. Bezpieczeństwo pracy zdalnej - praca na sprzęcie własnym lub służbowym.

Należy omówić zasady bezpieczeństwa dla pracy zdalnej.

1. Bezpieczeństwo zakupów oraz płatności w Internecie.

Należy omówić zasady bezpieczeństwa dla jednej z licznej grupy zagrożeń jakie są spowodowane handlem elektronicznym.

1. Zabezpieczenia prywatności.

Zwalczanie pożądanego śledzenia w Internecie np. w mediach społecznościowych itp.

1. Rozpoznawanie fałszywych informacji.

Rozpoznawanie fałszywych informacji. Zwalczenie dezinformacji.

1. Warsztat kontaktowy (w siedzibie Zamawiającego) :

2 x 45 minut – cyberbezpieczeństwo w ujęciu prawnym. Pierwsza godzina omówienie aspektów i studium przypadków. Druga rodzina podział na kilka grup i przeprocesowanie konkretnych symulowanych incydentów.

* Przegląd wyłudzanie danych osobowych za pomocą technik socjotechnicznych, czym jest socjotechnika i jak bronić się przed nią
* Przegląd funkcjonowania i rozpoznawanie zagrożeń typu: phishing i ransomware

1. **Uczestnik szkolenia online oraz kontaktowego lub osoba po odsłuchaniu cyklu szkoleń powinni otrzymać imienny certyfikat uczestnictwa w szkoleniu i jego zakresie.**