Załącznik nr 9C do SWZ – opis przedmiotu zamówienia

III część zamówienia\_szkolenia

**Szkolenia –** w siedzibie zamawiającego. Każde szkolenie czas trwania minimum 4 godziny dla każdej grupy. Realizowane w godzinach pracy zamawiającego. W formie stacjonarnej w oparciu o interaktywną relację z uczestnikami przy wykorzystaniu multimediów. Wymagane przygotowanie listy obecności na każdym szkoleniu

1. Cyberbezpieczeństwo - ochrona systemów informatycznych i zasobów JST. **(jedna grupa – 5 osób)**

* Rola informatyka w bezpieczeństwie IT.
* Omówienie zasad bezpiecznej pracy w systemach informatycznych w urzędzie
* Zarządzanie incydentami w Urzędzie

2. Cyberzagrożenia a ochrona danych osobowych i bezpieczeństwo informacji. **(dwie grupy – w sumie 36 osób)**

* Omówienie polityki ochrony danych osobowych w Urzędzie
* Polityka czystego biurka i ekranu.
* Omówienie polityki tworzenia bezpiecznych haseł
* Metody szyfrowania wiadomości i załączników

3. Najnowsze zagrożenia w sieci i ich konsekwencje. **(dwie grupy – w sumie 36 osób)**

* Jak działają wirusy?
* Phishing
* Zasada używania bankowości elektronicznej
* Odpowiedzialność za naruszenie zasad bezpieczeństwa informacji.

4. Bezpieczna praca zdalna i bezpieczna praca z dokumentem papierowym i elektronicznym. **(dwie grupy – w sumie 36 osób)**

* Omówienie przykładów spotykanych przez użytkowników oraz metod zabezpieczeń.
* Bezpieczne połączenie zdalne i praca w sieci
* Omówienie polityki bezpieczeństwa informacji

5. Bezpieczeństwo socjotechniczne, różne techniki inżynierii socjotechnicznej. **(dwie grupy – w sumie 36 osób)**

* Zasady bezpiecznego używania telefonu
* Jak należy identyfikować próby związane z kradzieżą informacji?
* Jakie są stosowane techniki i jak można się przed nimi uchronić?

6. Analiza ryzyka przetwarzania danych osobowych. **(dwie grupy – w sumie 36 osób)**

* Jak przeprowadzić analizę i ocenić ryzyko?
* Szacowanie ryzyka i konsekwencji jakie może ponieść organizacja

7. Ochrona danych osobowych w JST i sprawdzenie zgodności z RODO. **(dwie grupy – w sumie 36 osób)**

* Jak przeprowadzić audyt ochrony danych osobowych?
* Praktyczne aspekty stosowania RODO
* Odpowiedzialność i konsekwencje prawne.

8. Bezpieczeństwo i ochrona informacji w JST. **(dwie grupy – w sumie 36 osób)**

* Jak przeprowadzić audyt bezpieczeństwa w oparciu o Krajowe Ramy Interoperacyjności?
* Jak wdrażać działania zgodne z przepisami prawa: RODO, KRI, UKSC, aby zapewnić odpowiedni poziom bezpieczeństwa danych?

9. Dane osobowe w dobie COVID-19 i pracy zdalnej. **(dwie grupy – w sumie 36 osób)**

* Omówienie polityki ochrony danych osobowych w Urzędzie
* Zasady pracy zdalnej

10. Zarządzanie i konfigurowanie mechanizmów bezpieczeństwa w JST.  **(jedna grupa – 5 osób)**

* Technika zabezpieczeń sieciowych
* Inwentaryzacja oprogramowania
* Legalność oprogramowania a bezpieczeństwo.

**Po szkoleniu Zamawiający wymaga dostarczenia imiennych certyfikatów dla każdego uczestnika.**