Program szkolenia

1. Ogólne zasady ochrony informacji – OpSec
   - bezpieczeństwo fizyczne informacji,
   - ochrona informacji w ujęciu kognitywnym.
2. Postępowanie z dokumentami poza biurem
   - klasyfikacja i podział dokumentów z punktu widzenia stopnia ochrony i nośnika danych,
   - ogólne zasady postępowania z dokumentami prawnie chronionymi:
     - informacje niejawne,
     - tajemnica przedsiębiorstwa.
   - zabezpieczanie informacji:
     - bezpieczne koperty;
     - szyfrowanie nośników i komputerów przenośnych;
     - ochrona fizyczna;
     - korzystanie z telefonów komórkowych.
3. Organizacja spotkań biznesowych
   - przygotowanie rozmów handlowych,
   - organizacja briefingów w trakcie rozmów handlowych,
   - dokumentowanie spotkań - notatki pisemne,
   - dokumenty handlowe – ochrona w trakcie spotkań biznesowych,
   - praca w sieciach komputerowych, VPN (korzystanie z e-maila i social mediów),
   - nośniki elektroniczne.
4. Zachowania ryzykowne
   - profilowanie osób zajmujących kluczowe pozycje w firmie,
   - przyjmowanie prezentów,
   - spotkania nieoficjalne,
   - oficer bezpieczeństwa w firmie,
   - korzystanie z ekspertów zewnętrznych (np. tłumacze).
5. Wprowadzenie do analizy
   - informacja,
   - intelligence cycle (cykl analityczny/wywiadowczy),
   - źródła informacji – ocena,
   - podstawowe techniki analizy:
     - analiza powiązań,
     - chronologia zdarzeń,
     - analiza przepływów,
   - podstawowe narzędzia analityczne.
6. Wywiad cząstkowy – wprowadzenie
7. Podstawy komunikacji międzyludzkiej w ujęciu psychologicznym.
8. Podstawy negocjacji - negocjacje jako skuteczne narzędzie zdobywania przewagi informacyjnej.
9. Naruszenie bezpieczeństwa informacji.
   - przykłady zagrożeń w przypadku niestosowania zasad ochrony informacji,
   - identyfikacja incydentów bezpieczeństwa,
   - przykłady incydentów bezpieczeństwa,
   - odpowiedzialność służbowa i karna za naruszenie bezpieczeństwa różnych kategorii informacji.
10. Podsumowanie, pytania, dyskusja.