SYLABUS ECCC

MODUŁ: **VI M12** BEZPIECZEŃSTWO INFORMACJI

GRUPA KOMPETENCJI	KOMPETENCJE OBJĘTE STANDARDEM ECCC
1. Podstawy	1.1. Znaczenie informacji w organizacji. 1.2. Pojęciapodstawowe.Informacja,bezpieczeństwoinformacji,poufność, dostępność, dokładność, rozliczalność. 1.3. Zagrożenia. Klasyfikacja. 1.4. Bezpieczeństwo fizyczne, środowiskowe, zasobów ludzkich. 1.5. Poziomy bezpieczeństwa. 1.6. Plan bezpieczeństwa. 1.7. Audyt systemów informatycznych.
2. Inspekcja - analiza stanu bezpieczeństwa	2.1. Inwentaryzacja zasobów. 2.2. Ocena zagrożeń i strat. 2.3. Identyfikacja podatności na zagrożenia. 2.4. Strategie projektowania ochrony informacji. 2.5. Ocena stanu aktualnego. Testowanie.
3. Ochrona zasobów informacyjnych	3.1. Uświadomienie pracowników. 3.2. Kontrola dostępu. 3.3. Metody identyfikacji, uwierzytelnienia i autoryzacji. 3.4. Ochrona: dostępności, dokładności i poufności. 3.5. Modele i zasady rozliczalności. 3.6. Administrowanie bezpieczeństwem informacji.
4. Wykrywanie incydentów	4.1. Intruzi i metody ich działań. 4.2. Metody wykrywania incydentów.
5. Reakcja - zarządzanie incydentami	5.1. Planowanie działań. 5.2. Wykrycie oraz identyfikacja incydentu. 5.3. Reakcja na incydent: powiadamianie, ograniczanie. 5.4. Szacowanie szkód. 5.5. Odtwarzanie systemu po incydencie. 5.6. Odpowiedzialność.
6. Refleksja i poprawa	6.1. Dokumentowanie i ocena incydentów. 6.2. Modyfikacja planu bezpieczeństwa informacji. 6.3. Prawne aspekty bezpieczeństwa informacji.
7. Bezpieczeństwo informacji przesyłanych	7.1. Zagrożenia przesyłanych informacji. 7.2. Szyfrowanie danych. 7.3. Podpis elektroniczny i jego infrastruktura.