Do zadań Zespołu do spraw Ochrony Informacji Niejawnych należy:

1. zapewnienie ochrony informacji niejawnych w Komendzie poprzez stosowanie środków bezpieczeństwa fizycznego oraz zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w tym określenie poziomów zagrożeń;
2. zapewnienie ochrony systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne w tym realizowanie zadań inspektora bezpieczeństwa teleinformatycznego (BTI);
3. kontrola i nadzór nad niejawnymi systemami teleinformatycznymi (TI);
4. kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w komórkach organizacyjnych Komendy;
5. okresowa kontrola ewidencji, materiałów i obiegu dokumentów niejawnych w Komendzie;
6. opracowywanie i aktualizowanie planu ochrony informacji niejawnych w Komendzie i nadzorowanie jego realizacji;
7. opracowywanie i aktualizowanie planu ochrony informacji niejawnych w razie wprowadzenia stanu nadzwyczajnego i nadzorowanie jego realizacji;
8. szkolenie policjantów i pracowników Komendy w zakresie ochrony informacji niejawnych według zasad określonych w ustawie o ochronie informacji niejawnych;
9. prowadzenie postępowań sprawdzających i kontrolnych wobec policjantów i pracowników Komendy oraz wobec kandydatów do służby lub pracy;
10. prowadzenie procedury wydawania upoważnień do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”;
11. prowadzenie aktualnego wykazu osób posiadających uprawnienia do dostępu do informacji niejawnych oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
12. prowadzenie Kancelarii Tajnej, w tym:
13. obsługa kancelaryjna Komendy w zakresie rejestracji i dystrybucji dokumentów niejawnych,
14. prowadzenie ewidencji i zbioru niejawnych przepisów służbowych,
15. powielanie dokumentów niejawnych,
16. nadzór nad obiegiem dokumentów niejawnych w Komendzie,
17. bieżące rozliczanie policjantów i pracowników Komendy z posiadanych dokumentów niejawnych;
18. prowadzenie Składnicy Akt, w tym:
19. przyjmowanie, ewidencjonowanie, opracowywanie, przechowywanie oraz zabezpieczanie zasobu archiwalnego,
20. udostępnianie materiałów z zasobu archiwalnego uprawnionym podmiotom,
21. udzielanie informacji z posiadanego zasobu archiwalnego uprawnionym podmiotom,
22. wydawanie zaświadczeń, uwierzytelnionych odpisów, wypisów, wyciągów i kserokopii dokumentów,
23. brakowanie dokumentacji niearchiwalnej kat. „B” oznaczonej symbolem „B” lub „BE” z zasobu archiwalnego Komendy,
24. kształtowanie narastającego zasobu archiwalnego Komendy,
25. nadzór nad brakowaniem dokumentacji niearchiwalnej kat „B” oznaczonej symbolem „BC” przez komórki organizacyjne, poprzez analizę protokołów oraz kontrolę kwalifikacji brakowanych dokumentów przed wydaniem zgody na jej zniszczenie,
26. przeprowadzanie okresowych inwentaryzacji zasobu archiwalnego Komendy;
27. opracowywanie decyzji wewnętrznych i procedur regulujących funkcjonowanie pionu ochrony w Komendzie oraz decyzji w sprawie zniesienia lub zmiany klauzuli tajności w ramach przeglądów dokumentów niejawnych;
28. podejmowanie działań zmierzających do wyjaśnienia okoliczności naruszenia przepisów o ochronie informacji niejawnych;
29. współpraca z KWP w Lublinie, organami organizacji rządowej i samorządowej, instytucjami państwowymi oraz innymi jednostkami organizacyjnymi w zakresie ochrony informacji niejawnych;
30. przyjmowanie i przechowywanie oświadczeń o stanie majątkowym od policjantów oraz udostępnianie upoważnionym osobom w celu dokonania analizy;
31. wykonywanie zadań administratora bezpieczeństwa informacji (ABI) w sposób określony w ustawie o ochronie danych osobowych i przepisach wykonawczych, w tym:
32. zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
	* sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (w trybie sprawdzeń planowych, doraźnych oraz w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora Ochrony Danych Osobowych) oraz opracowanie w tym zakresie sprawozdań dla administratora danych,
	* nadzorowanie opracowania i aktualizowania dokumentacji bezpieczeństwa (w postaci polityki bezpieczeństwa ochrony danych osobowych oraz instrukcji zarządzania systemem informatycznym) oraz przestrzegania zasad w niej określonych,
	* zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
33. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, które są zwolnione z obowiązku rejestracji na podstawie ustawy oraz rejestrowanie u GIODO zbiorów danych podlegających obowiązkowi rejestracji;
34. wydawanie opinii, pouczeń i instrukcji w sprawach dotyczących ochrony i przetwarzania danych osobowych.