

**DECYZJA Nr 74/MON**  
**MINISTRA OBRONY NARODOWEJ**

z dnia 27 marca 2013 r.

**w sprawie eksploatacji niejawnego systemu teleinformatycznego PL\_NS NOAN**

Na podstawie § 1 pkt 11 lit. f oraz § 2 pkt 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426) ustala się, co następuje:

1. Użyte w decyzji określenia oznaczają:
  - 1) dokumentacja bezpieczeństwa systemu teleinformatycznego – dokumentację obejmującą następujące elementy: RA (ang. Risk Assessment), SSRS (ang. Specific System Requirement Statement), SIRS (ang. Specific Interconnection Requirement Statement), SecOPs (ang. Security Operations Procedures), LUBST (pol. Lokalne Uwarunkowania Bezpieczeństwa Systemu Teleinformatycznego), ST&E Plan (ang. Security Testing and Evaluation Plan);
  - 2) FAS (ang. Functional Area Service) – system informatyczny lub usługę funkcjonującą w systemie teleinformatycznym PL\_NS NOAN;
  - 3) jednostka organizacyjna – Ministerstwo Obrony Narodowej, jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną oraz Służbę Kontrwywiadu Wojskowego i Służbę Wywiadu Wojskowego;
  - 4) kierownik jednostki organizacyjnej lub komórki organizacyjnej – dowódcę, szefa, dyrektora, komendanta lub inną osobę kierującą całokształtem działalności jednostki organizacyjnej lub komórki organizacyjnej, w której funkcjonuje system PL\_NS NOAN lub są planowane do uruchomienia jego elementy;
  - 5) komórka organizacyjna – komórkę organizacyjną Ministerstwa Obrony Narodowej w rozumieniu § 2 pkt 5 regulaminu organizacyjnego Ministerstwa Obrony Narodowej, stanowiącego załącznik do zarządzenia Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej (Dz. Urz. MON Nr 21, poz. 270, z późn. zm.<sup>1)</sup>);
  - 6) krajowa władza akredytacyjna – Służbę Kontrwywiadu Wojskowego;

---

<sup>1)</sup> Zmiany wymienionego zarządzenia zostały ogłoszone w Dz. Urz. MON z 2007 r. Nr 4, poz. 38, Nr 6, poz. 73, Nr 17, poz. 176 i Nr 21, poz. 209, z 2008 r. Nr 8, poz. 85, Nr 15, poz. 188, Nr 20, poz. 260 i Nr 23, poz. 287, z 2009 r. Nr 2, poz. 17, z 2010 r. Nr 10, poz. 106 i Nr 23, poz. 304, z 2011 r. Nr 5, poz. 54 oraz z 2012 r. poz. 106, 307, 313 i 363.

- 7) NATO – Organizacja Traktatu Północnoatlantyckiego;
  - 8) NS WAN (ang. NATO Secret Wide Area Network) – rozległą sieć teleinformatyczną do przetwarzania informacji do klauzuli NATO SECRET;
  - 9) organizator systemu teleinformatycznego – kierownika jednostki organizacyjnej organizującej system teleinformatyczny lub upoważnionego przez niego kierownika komórki organizacyjnej;
  - 10) PL\_NS NOAN (ang. Polish NATO Secret NATO Office Automation Network – System Automatyzacji Prac Biurowych) – Polską Sieć Automatyzacji Procesów Biurowych NATO o klauzuli NATO SECRET;
  - 11) system teleinformatyczny – system teleinformatyczny w rozumieniu art. 2 pkt 6 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
  - 12) ustawa – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
2. System teleinformatyczny PL\_NS NOAN zapewnia dołączenie innych systemów teleinformatycznych funkcjonujących w Polskim Segmentie Sieci NS WAN, w tym usług i aplikacji FAS, a także systemów teleinformatycznych będących poza obszarem odpowiedzialności resortu obrony narodowej, zapewniając tym samym bezpośrednią wymianę informacji niejawnych do klauzuli NATO SECRET włącznie. Dołączenie innych systemów teleinformatycznych odbywa się na bazie porozumienia technicznego podpisanego przez organizatorów systemów teleinformatycznych.
  3. Dyrektor Departamentu Informatyki i Telekomunikacji:
    - 1) pełni rolę organizatora systemu teleinformatycznego PL\_NS NOAN;
    - 2) koordynuje działania związane z planowaniem, eksploatacją i wycofaniem systemu teleinformatycznego PL\_NS NOAN;
    - 3) zapewnia współpracę z właściwymi organami odpowiedzialnymi za zarządzanie bezpieczeństwem systemu NS WAN w NATO.
  4. Dyrektor Departamentu Ochrony Informacji Niejawnych – Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych:
    - 1) pełni rolę Pełnomocnika Ochrony Informacji Niejawnych dla Organizatora Systemu Teleinformatycznego PL\_NS NOAN;
    - 2) powołuje zespół, w celu opracowania Analizy Ryzyka na potrzeby dokumentacji bezpieczeństwa systemu teleinformatycznego PL\_NS NOAN.
  5. Szef Zarządu Planowania Systemów Dowodzenia i Łączności – P6 Sztabu Generalnego Wojska Polskiego:
    - 1) określa według potrzeb wynikających z planu użycia Sił Zbrojnych Rzeczypospolitej Polskiej zasady operacyjnego wykorzystania systemu PL\_NS NOAN na czas pokoju, kryzysu i wojny;
    - 2) opiniuje wnioski w sprawie dołączenia do systemu PL\_NS NOAN nowych lokalizacji oraz wdrożenia nowych systemów informatycznych lub usług w systemie PL\_NS NOAN.
  6. Szef Służby Kontrywiadu Wojskowego:
    - 1) udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego PL\_NS NOAN;
    - 2) zapewnia dokumenty kryptograficzne na potrzeby funkcjonowania systemu teleinformatycznego PL\_NS NOAN;
    - 3) realizuje w odniesieniu do systemu teleinformatycznego PL\_NS NOAN zadania, o których mowa w art. 10 ustawy.

7. Komendant Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych:
  - 1) pełni funkcję operacyjnej władzy bezpieczeństwa w zakresie zabezpieczenia kryptograficznego systemu teleinformatycznego PL\_NS NOAN;
  - 2) sprawuje nadzór nad prawidłową eksploatacją systemu ochrony kryptograficznej;
  - 3) wnioskuje do organizatora systemu o modernizację systemu ochrony kryptograficznej;
  - 4) odpowiada za opracowanie dokumentacji bezpieczeństwa systemu teleinformatycznego PL\_NS NOAN;
  - 5) odpowiada za przygotowanie planu testów bezpieczeństwa teleinformatycznego systemu PL\_NS NOAN oraz planu testów bezpieczeństwa dla połączeń międzysystemowych dla systemów do niego dołączanych;
  - 6) odpowiada za przygotowanie raportów końcowych z przeprowadzonych testów i przesłanie ich do władzy akredytacyjnej systemu;
  - 7) wyznacza Oficera Bezpieczeństwa Systemu dla systemu teleinformatycznego PL\_NS NOAN – będącego odpowiednikiem ang. System Security Officer (SSO) w systemie NS WAN z zakresem obowiązków wynikającym z dokumentacji bezpieczeństwa systemu teleinformatycznego PL\_NS NOAN;
  - 8) zaopatruje jednostki organizacyjne w dokumenty kryptograficzne dla systemu teleinformatycznego PL\_NS NOAN;
  - 9) odpowiada za skompletowanie, przygotowanie i dostarczenie do Służby Kontrwywiadu Wojskowego dokumentu o nazwie „NS WAN System Interconnection Security Requirement Statement (SISRS) Annex B”, którego przyjęcie jest warunkiem podłączenia PL\_NS NOAN do systemów NATO;
  - 10) odpowiada za wsparcie techniczne systemu reagowania na incydenty komputerowe resortu obrony narodowej zgodnie z decyzją 357/MON z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. MON Nr 16, poz. 205).
8. Szef Centrum Wsparcia Teleinformatycznego Sił Zbrojnych:
  - 1) zapewnia funkcjonowanie systemu PL\_NS NOAN i usług bazowych, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego z uwzględnieniem centralnej organizacji zarządzania bezpieczeństwem informacji niejawnych „central security managment”;
  - 2) zabezpiecza działanie punktu dostępowego – PoP (ang. Point of Presence) do sieci NS WAN;
  - 3) zapewnia stały nadzór i monitorowanie systemu w trybie 24 godzinnym, w zakresie prawidłowego funkcjonowania warstwy transmisyjnej PL\_NS NOAN;
  - 4) wyznacza administratora systemu PL\_NS NOAN stosownie do dokumentacji bezpieczeństwa systemu teleinformatycznego;
  - 5) odpowiada za zarządzanie ochroną kryptograficzną systemu PL\_NS NOAN;
  - 6) koordynuje proces wymiany urządzeń i oprogramowania w systemie PL\_NS NOAN;
  - 7) odpowiada za przeprowadzenie testów bezpieczeństwa teleinformatycznego systemu PL\_NS NOAN oraz testów bezpieczeństwa dla połączeń

międzysystemowych i koordynuje powyższe przedsięwzięcia w poszczególnych lokalizacjach systemu;

- 8) wyznacza administratora lokalnego systemu dla komórek organizacyjnych oraz jednostek organizacyjnych znajdujących się w rejonie odpowiedzialności Centrum Wsparcia Teleinformatycznego Sił Zbrojnych na obszarze Garnizonu Warszawa.
9. Kierownicy jednostek organizacyjnych realizują następujące zadania:
  - 1) wyznaczą osoby funkcyjne będące personelem bezpieczeństwa systemu, realizujące zadania wynikające z obowiązującej dokumentacji bezpieczeństwa dla PL\_NS NOAN:
    - a) **HQSO** (ang. Headquater Security Officer) pełnioną przez pełnomocnika ochrony informacji niejawnych,
    - b) **SiteSO** (ang. Site Security Officer) pełnioną przez inspektora bezpieczeństwa teleinformatycznego,
    - c) lokalnego administratora systemu – **LSA** (ang. Local System Administrator), z zastrzeżeniem pkt 9 ust. 8,
    - d) **COMSEC** (ang. Communication Security Officer) pełnioną przez oficera bezpieczeństwa systemów łączności i informatyki,
    - e) oficera bezpieczeństwa terminala – **TASO** (ang. Terminal Area Security Officer).
  - 2) sprawują nadzór nad opracowaniem lokalnej dokumentacji bezpieczeństwa w zakresie wynikającym z dokumentacji ogólnosystemowej systemu teleinformatycznego PL\_NS NOAN;
  - 3) wnioskuje do organizatora systemu teleinformatycznego o wyrażenie zgody na dołączenie do systemu PL\_NS NOAN nowej lokalizacji oraz wdrożenie nowych systemów informatycznych lub usług;
  - 4) zgłaszają do organizatora systemu teleinformatycznego potrzeby w zakresie modernizacji sprzętu i oprogramowania systemu PL\_NS NOAN;
  - 5) odpowiadają za przeprowadzenie testów bezpieczeństwa systemu w ramach jednostki organizacyjnej koordynowanych przez administratora systemu;
  - 6) zapewniają bezpieczeństwo eksploatowanym elementom systemu teleinformatycznego PL\_NS NOAN stosownie do poziomu wymaganego dokumentacją ogólnosystemową.
10. Kierownicy komórek organizacyjnych realizują następujące zadania:
  - 1) wyznaczają oficera bezpieczeństwa terminala – **TASO** (ang. Terminal Area Security Officer), realizującego zadania wynikające z zatwierdzonej dokumentacji bezpieczeństwa dla PL\_NS NOAN;
  - 2) sprawują nadzór nad opracowaniem lokalnej dokumentacji bezpieczeństwa w zakresie wynikającym z dokumentacji ogólnosystemowej systemu teleinformatycznego PL\_NS NOAN;
  - 3) wnioskuje do organizatora systemu teleinformatycznego o wyrażenie zgody na dołączenie do systemu PL\_NS NOAN nowej lokalizacji oraz wdrożenie nowych systemów informatycznych lub usług;
  - 4) zapewniają bezpieczeństwo eksploatowanym elementom systemu teleinformatycznego PL\_NS NOAN stosownie do poziomu wymaganego dokumentacją ogólnosystemową.
11. Szef Sztabu Generalnego Wojska Polskiego wyda dokumenty rozkazodawcze niezbędne do właściwego funkcjonowania PL\_NS NOAN.

12. Traci moc decyzja Nr 26/DOW/P-6 Ministra Obrony Narodowej z dnia 2 kwietnia 2001 r. w sprawie rozpoczęcia eksploatacji niejawnego systemu wymiany informacji z dowództwami i państwami członkowskimi Organizacji Traktatu Północnoatlantyckiego.
13. Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Obrony Narodowej: *T. Siemoniak*