



## WYSTĄPIENIE POKONTROLNE

Na podstawie §4 i §13 ust.1 oraz §8 ust.1 załącznika do Decyzji Nr 65 Ministra Spraw Wewnętrznych z dnia 31 maja 2012 r. w sprawie wprowadzenia do stosowania wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych (Dz. Urz. MSW z 2012 r., poz. 43, z późn. zm.) zespół kontrolny przeprowadził w Wydziale Granicznym Nadbużańskiego Oddziału Straży Granicznej czynności kontrolne.

W związku z zakończeniem czynności kontrolnych w Wydziale Granicznym NOSG, stosownie do §35 cytowanego powyżej aktu prawnego przekazuję Panu Naczelnikowi wystąpienie pokontrolne.

### I. Nazwa i adres podmiotu kontrolowanego, imię i nazwisko kierownika podmiotu kontrolowanego:

Wydział Graniczny Nadbużańskiego Oddziału Straży Granicznej,  
ul. Trubakowska 2, 22-100 Chełm,  
kpt. SG Rafał BUDA

### II. Imię, nazwisko i stanowisko służbowe kontrolerów:

Kierownik zespołu kontrolnego:

- mjr SG Dariusz GREGUŁA – kierownik Sekcji Ochrony Informacji Wydziału Ochrony Informacji Nadbużańskiego Oddziału Straży Granicznej – upoważnienie nr 27/WOI/23 z dnia 11 września 2023 r.

Członkowie zespołu kontrolnego:

- plut. SG Artur SIKORA – starszy specjalista – inspektor bezpieczeństwa teleinformatycznego Sekcji Ochrony Informacji Wydziału Ochrony Informacji Nadbużańskiego Oddziału Straży Granicznej – upoważnienie nr 28/WOI/23 z dnia 11 września 2023 r.
- Marcin MIŚKIEWICZ – starszy specjalista – inspektor bezpieczeństwa teleinformatycznego Sekcji Ochrony Informacji Wydziału Ochrony Informacji Nadbużańskiego Oddziału Straży Granicznej – upoważnienie nr 29/WOI/23 z dnia 11 września 2023 r.

### III. Data rozpoczęcia i zakończenia czynności kontrolnych:

Czynności kontrolne przeprowadzono w dniach 05.10.2023 r., 10.10.2023 r. i 12.10.2023 r.

#### IV. Przedmiot kontroli:

Kontrola zgodności funkcjonowania akredytowanych systemów teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji:

1. Systemu [REDACTED]
2. Systemu [REDACTED]
3. Systemu [REDACTED]
4. Systemu [REDACTED]
5. Sieci [REDACTED]
6. Systemu [REDACTED]

w szczególności:

- a) zabezpieczenie globalnego i lokalnego środowiska bezpieczeństwa,
- b) konfiguracji elektronicznego środowiska bezpieczeństwa,
- c) dostępu użytkowników do systemu,
- d) zgodności zainstalowanego oprogramowania z dokumentacją bezpieczeństwa,
- e) aktualność dokumentacji bezpieczeństwa i dokumentacji pomocniczej.

#### V. Okres objęty kontrolą:

Stan bieżący.

#### VI. Ocena skontrolowanej działalności, ze wskazaniem ustaleń, na których została oparta:

Zespół kontrolny w trakcie przeprowadzonych czynności kontrolnych stwierdził co następuje:

1. System [REDACTED]

– stanowisko nr [REDACTED]

2. System [REDACTED]

– stanowisko [REDACTED]

3. System [REDACTED]

– stanowisko [REDACTED]

Kontroli podlegały następujące zagadnienia umożliwiające ocenę działalności komórki kontrolowanej w zakresie:

- 1) *prawidłowości podłączenia (lub braku podłączenia) kontrolowanych stanowisk do sieci teleinformatycznej* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 2) *terminowego przeglądu okablowania przez lokalnych administratorów* – stwierdzono wpisy potwierdzające fakt dokonania przeglądu okablowania,
- 3) *zabezpieczenia stanowisk plombami* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 4) *rejestracji informatycznych nośników danych i materiałów wykorzystywanych w systemie* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 5) *prawidłowości konfiguracji ustawień BIOS* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 6) *prawidłowości konfiguracji systemu operacyjnego* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 7) *instalacji i konfiguracji oprogramowania antywirusowego* – stwierdzono zainstalowane oprogramowanie antywirusowe oraz jego poprawną konfigurację,
- 8) *aktualności oprogramowania antywirusowego* – stwierdzono termin aktualizacji zgodny z dokumentacjami bezpieczeństwa,
- 9) *zgodności zainstalowanego oprogramowania użytkowego z dokumentacją bezpieczeństwa* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 10) *założenia i usunięcia kont na podstawie Zleceń nadania/cofnięcia uprawnień* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

- 12) wyznaczenia osób funkcyjnych odpowiedzialnych za bezpieczeństwo systemu oraz posiadanie przez nich odpowiednich poświadczeń bezpieczeństwa i szkoleń oraz ważności poświadczeń bezpieczeństwa użytkowników oraz posiadanie przez nich odpowiednich szkoleń – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 13) posiadania przez lokalnych administratorów podpisanych oświadczeń przez użytkowników systemu o zapoznaniu się z Procedurami Bezpiecznej Eksploatacji – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 14) aktualności prowadzenia „Dziennika działań administratora” przez lokalnych administratorów – nie stwierdzono braku wpisów potwierdzających fakt wykonania prac administracyjnych lub związanych z bezpieczeństwem stanowisk,
- 15) przeprowadzenia analizy logów systemowych przez lokalnych administratorów – stwierdzono wpisy potwierdzające fakt przeprowadzenia analizy logów systemowych przez lokalnego administratora,
- 16) aktualizacji „Opisów stanowisk” – nie stwierdzono błędnych lub nieaktualnych wpisów,
- 17) posiadania przez lokalnych administratorów niezbędnej dokumentacji bezpieczeństwa oraz dokumentacji pomocniczej – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa.

W wyniku przeprowadzonych czynności kontrolnych zagadnień zawartych w pkt. od 1 do 17 nie stwierdzono nieprawidłowości w stosunku do kontrolowanych stanowisk systemów teleinformatycznych.

Stan funkcjonowania stanowisk systemu [REDAKTOWANE] oraz [REDAKTOWANE] wskazanych w części VI pkt 1, 2 oraz 3 jest zgodny z dokumentacjami bezpieczeństwa.

**W związku z powyższym kontrolowane zagadnienia należy ocenić pozytywnie.**

4. System [REDAKTOWANE]  
– stanowisko [REDAKTOWANE]
5. System [REDAKTOWANE]  
– stanowisko [REDAKTOWANE]
6. System [REDAKTOWANE]  
– stanowisko [REDAKTOWANE]

Kontroli podlegały następujące zagadnienia umożliwiające ocenę działalności komórki kontrolowanej w zakresie:

- 1) prawidłowości podłączenia (lub braku podłączenia) kontrolowanych stanowisk do sieci teleinformatycznej – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 2) terminowego przeglądu okablowania przez lokalnego administratora – stwierdzono wpisy potwierdzające fakt dokonania przeglądu okablowania,
- 3) zabezpieczenia stanowisk plombami – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 4) rejestracji informatycznych nośników danych i materiałów wykorzystywanych w systemie – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 5) założenia i usunięcia kont na podstawie Zleceń nadania/cofnięcia uprawnień – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 6) zabezpieczeń globalnego i lokalnego środowiska bezpieczeństwa – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 7) wyznaczenia osób funkcyjnych odpowiedzialnych za bezpieczeństwo systemu oraz posiadanie przez nich odpowiednich poświadczeń bezpieczeństwa i szkoleń oraz ważności poświadczeń bezpieczeństwa użytkowników oraz posiadanie przez nich odpowiednich szkoleń – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 8) posiadania przez lokalnego administratora podpisanych oświadczeń przez użytkowników systemu o zapoznaniu się z Procedurami Bezpiecznej Eksploatacji – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
- 9) aktualności prowadzenia „Dziennika działań administratora” przez lokalnego administratora – nie stwierdzono braku wpisów potwierdzających fakt wykonania prac administracyjnych lub związanych z bezpieczeństwem stanowisk,

