BIURO SPRAW WEWNĘTRZNYCH
STRAŻY GRANICZNEJ

Warszawa, dnia 28.06.2022 r.

Egz. nr 1

SW-OI.0910.1.2022

Naczelnik Wydziału II
Biura Spraw Wewnętrznych
Straży Granicznej
płk SG Małgorzata WIĄCEK

WYSTĄPIENIE POKONTROLNE

z kontroli planowej w trybie zwykłym, ujętej w **Planie kontroli informacji niejawnych do realizacji przez Wydział Ochrony Informacji Biura Spraw Wewnętrznych Straży Granicznej w 2022 roku** z dnia 14 grudnia 2021 r. (SW-OI.0930.4.2021).

Kontrola została przeprowadzona na podstawie wytycznych, stanowiących załącznik 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*[1].

I. Podmiot kontrolowany.

Wydział II Biura Spraw Wewnętrznych Straży Granicznej, 02-148 Warszawa, ul. Komitetu Obrony Robotników 23.

Funkcję kierownika podmiotu kontrolowanego w okresie objętym kontrolą pełniła:

- **płk SG Małgorzata WIĄCEK** – Naczelnik Wydziału II BSWSG.

II. Imię i nazwisko, stanowisko służbowe kontrolerów, nazwa komórki kontroli oraz nr i data upoważnienia do kontroli z uwzględnieniem zmian w okresie prowadzenia kontroli.

[1] (Dz. Urz. Min. Spraw Wew. poz. 43, z późn. zm.)

Zespół kontrolny w składzie:
kierownik zespołu:

- **por. SG** [redacted] – zastępca naczelnika Wydziału Ochrony Informacji BSWSG, upoważnienie nr 79 z dnia 12 kwietnia 2022 r.

członkowie zespołu:

- **chor. SG** [redacted] – starszy specjalista Wydziału Ochrony Informacji BSWSG, upoważnienie nr 82 z dnia 12 kwietnia 2022 r.
- **chor. szt. SG** [redacted] – starszy specjalista Wydziału Ochrony Informacji BSWSG, upoważnienie nr 81 z dnia 12 kwietnia 2022 r.
- **sierż. szt. SG** [redacted] – specjalista w Kancelarii Tajnej Wydziału Ochrony Informacji BSWSG, upoważnienie nr 80 z dnia 12 kwietnia 2022 r.

III. Data rozpoczęcia i zakończenia czynności kontrolnych w podmiocie kontrolowanym, z wymienieniem przerw w kontroli.

Czynności kontrolne przeprowadzono w terminie 11.04-08.06.2022 r.

IV. Zakres przedmiotowy i okres objęty kontrolą.

1. Przedmiotem kontroli było:

   a) okresowa kontrola ewidencji, materiałów i obiegu dokumentów niejawnych poprzez sprawdzenie zgodności stanu faktycznego losowo wybranych materiałów niejawnych ze stanem ewidencyjnym,
   b) prowadzenie urządzeń ewidencyjnych:
   - kompletność zapisów potwierdzenie pobrania / zwrotu dokumentu;
   - dokumentowanie wybrakowania dokumentów;
   - potwierdzenie faktu włączenia dokumentu do teczki;
   - dokumentowanie ujęcia dokumentu na ewidencji innego urządzenia ewidencyjnego;
   - dokumentowanie wysłania dokumentu,
   c) ochrona fizyczna Wydziału II BSWSG
   - dokumentowanie ochrony obiektu i sposobu jej realizacji; pobierania i zdawania kluczy, zasady wejść i wyjść, przyjmowanie interesantów, wydzielenie stref ochronnych, system CCTV, SKD,
   d) realizacja obsługi pocztowej i ochrony przesyłek pocztowych.
   e) bezpieczeństwo TI w zakresie wykonywania dokumentów niejawnych:
   - świadectwa akredytacji bezpieczeństwa systemu TI;
   - dokumentacja Lokalnego Administratora Systemu lub operatora systemu;
   - nadawanie uprawnień użytkowników do systemu TI.
   f) sprawdzenie i zebranie szczegółowych informacji dotyczących zastosowanych środków bezpieczeństwa określonych w dokumentacji bezpieczeństwa [redacted] oraz potwierdzenie ich zgodności ze stanem faktycznym,
   g) bezpieczeństwo TI w zakresie wykonywania dokumentów niejawnych:
   - świadectwa akredytacji bezpieczeństwa systemu TI;
   - dokumentacja Lokalnego Administratora Systemu lub operatora systemu;
   - nadawanie uprawnień użytkowników do systemu TI,

h) realizacja obsługi pocztowej i ochrony przesyłek pocztowych.

2. Okres objęty kontrolą od 27 stycznia 2018 r. do 31 grudnia 2020 r.

V. Cele kontroli.

1. Sprawdzenie ewidencji, materiałów i obiegu dokumentów niejawnych oraz zgodności stanu faktycznego materiałów niejawnych ze stanem ewidencyjnym na podstawie urządzeń ewidencyjnych.
2. Zapewnienie zgodnego z obowiązującymi przepisami postępowania z dokumentami niejawnymi.
3. Eliminowanie stwierdzonych niedociągnięć i nieprawidłowości w zakresie przetwarzania dokumentów niejawnych.
4. Formułowanie wniosków i zaleceń w sprawie doskonalenia systemu ochrony informacji niejawnych.
5. Wyrabianie u wykonawców właściwych nawyków w postępowaniu z dokumentami niejawnymi.
6. Weryfikacja i bieżąca kontrola zgodności funkcjonowania stanowisk dostępowych [redacted] ze szczególnymi wymaganiami bezpieczeństwa i przestrzegania procedur bezpiecznej eksploatacji oraz opisem lokalizacji stanowisk dostępowych ww. systemów teleinformatycznych.
7. Sprawdzenie ewidencji informatycznych nośników danych wykorzystywanych w systemach, tj. porównanie stanu faktycznego ze stanem ewidencyjnym na podstawie urządzeń ewidencyjnych.
8. Eliminowanie stwierdzonych niedociągnięć i nieprawidłowości w zakresie przetwarzania informacji niejawnych na akredytowanych stanowiskach teleinformatycznych.
9. Wyrabianie u użytkowników akredytowanych systemów teleinformatycznych właściwych nawyków, w tym stosowania dobrych praktyk w trakcie użytkowania akredytowanych systemów teleinformatycznych.
10. Ujawnienie ewentualnych nieprawidłowości i przyczyn ich powstania oraz osób za nie odpowiedzialnych.

VI. Ocena skontrolowanej działalności ze wskazaniem ustaleń, na których została oparta. Zakres przyczyny i skutki stwierdzonych nieprawidłowości oraz wskazanie osób za nie odpowiedzialnych.

Realizację zadań objętych zakresem kontroli oceniono **pozytywnie.** Powyższą ocenę sformułowano w oparciu o kontrolę ochrony informacji niejawnych w zakresie ewidencji i obiegu dokumentów/materiałów o klauzuli „poufne", „tajne" i „ściśle tajne".

Zespół kontrolny **pozytywnie** ocenia stan przestrzegania przepisów o ochronie informacji niejawnych, w zakresie ewidencji materiałów i obiegu dokumentów /materiałów niejawnych.

Powyższą ocenę sformułowano w oparciu o:

1. kontrolę dokumentów/materiałów będących na stanie Wydziału II BSWSG oraz niżej wymienionych urządzeń ewidencyjnych prowadzonych w Wydziale II BSWSG:
   a) Książka rejestracji kart E-15, wg Rdet SW-PF-10/18,

b) Książka rejestracji kart E-15, wg Rdet SW-PF-11/18,
c) Dziennik ewidencyjny szyfrofaksów wchodzących, wg Rdet SW-Z-12/18,
d) Dziennik ewidencyjny szyfrofaksów wychodzących, wg Rdet SW-Z-26/18,
e) Dziennik ewidencyjny szyfrofaksów wchodzących, wg Rdet SW-Z-30/18,
f) Dziennik ewidencyjny szyfrofaksów wychodzących, wg Rdet SW-Z-31/18,
g) Dziennik ewidencyjny szyfrofaksów wchodzących, wg Rdet SW-Z-9/19,
h) Dziennik ewidencyjny szyfrofaksów wchodzących, wg Rdet SW-Z-11/20,
i) Książka rejestracji kart E-15- wychodzących, wg Rdet SW-PF-32/18,
j) Ewidencja dokumentów posiadanych przez BSWSG – dokumenty legalizacyjne, wg Rdet SW-PF-33/18,
k) Dziennik rejestracji osób, wg Rdet SW-PF-34/18,
l) Dziennik rejestracji TEO, wg Rdet SW-PF-35/18,
m) Dziennik rejestracji, wg Rdet SW-00-36/18,
n) Dziennik ewidencyjny szyfrofaksów wchodzących, wg Rdet SW-Z-7/20,
o) Dziennik ewidencyjny szyfrofaksów wychodzących, wg Rdet SW-Z-8/20,
p) Książka rejestracji kart E-15, wg Rdet SW-PF-9/20,

2. kontrolę niżej wymienionych urządzeń ewidencyjnych prowadzonych w Kancelarii Tajnej BSWSG:
a) Rejestr dzienników ewidencji i teczek BSWSG,
b) Skorowidz Rejestrów BSWSG, wg Rdet SW-9/18,
c) Dziennik ewidencyjny korespondencji wchodzącej - poufne, wg Rdet SW-Z-17/18,
d) Dziennik ewidencyjny korespondencji wychodzącej - poufne, wg Rdet SW-Z-18/18,
e) Dziennik ewidencyjny korespondencji wchodzącej / wychodzącej - tajne, wg Rdet SW-Z-19/18,
f) Dziennik ewidencyjny korespondencji wchodzącej / wychodzącej - ściśle tajne, wg Rdet SW–Z–20/18,
g) Dziennik ewidencyjny – dokumenty własne BSWSG, wg Rdet SW-Z-21/18,
h) Dziennik ewidencyjny – dokumenty własne BSWSG – poufne, wg Rdet SW-Z-/19,
i) Dziennik ewidencyjny korespondencji wchodzącej - poufne, wg Rdet SW-Z-7/19,
j) Dziennik ewidencyjny korespondencji wchodzącej – poufne, wg Rdet SW-Z-2/2020,
k) Dziennik ewidencyjny korespondencji wychodzącej - poufne, wg Rdet SW-Z-3/2020,
l) Dziennik ewidencyjny – dokumenty własne BSWSG, wg Rdet SW-Z-4/2020,
m) Rejestr wydanych przedmiotów, wg Rdet SW-29/18,
n) Wykazy przesyłek nadanych, sprawdzono w oparciu o wykazy BSWSG z lat 2018, 2019 i 2020,
o) Wykaz osób dopuszczonych do dostępu do informacji niejawnych BSWSG, RWD 24-SW-4/18.

W wyniku kontroli ustalono co następuje:

- stwierdzono zgodność stanu faktycznego dokumentów niejawnych ze stanem ewidencyjnym w okresie objętym kontrolą w urządzeniach ewidencyjnych wykorzystywanych w Wydziale II BSWSG oraz w Kancelarii Tajnej BSWSG,
- nie stwierdzono przypadku udostępnienia dokumentu niejawnego funkcjonariuszowi nie posiadającemu stosownego poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych,

- osoby wykonujące czynności kancelaryjne w Wydziale II BSWSG, w zakresie ewidencjonowania szyfrofaksów wchodzących i wychodzących oraz rejestrowania dokumentów dotyczących próśb o udzielenie informacji, a także odpowiedzi w przedmiotowych kwestiach, w tym przesyłanych w formie szyfrofaksów, posiadały stosowne upoważnienia do wykonywania ww. czynności,
- obsługę pocztową dla podmiotu kontrolowanego wykonują pracownicy Kancelarii Tajnej BSWSG. W okresie objętym kontrolą stwierdzono zgodność zapisów w urządzeniach ewidencyjnych z wykazami przesyłek nadanych. Sprawdzono losowo wybrane wykazy przesyłek z 2018 roku:
  - 47 poz. 1: SW-EA-PF-9/11/18; SW-EA-PF-7/11/18;
  - 145 poz. 2: SW-EA-PF-55/5/18;
  - 189 poz. 1: SW-EA-PF-65/5/18;
  - 270 poz. 6: SW-EA-PF-91/4/18;
  - 328 poz. 2: SW-EA-PF-110/4/18,

  z 2019 roku:
  - 224 poz. 1: SW-EA-PF-112/4/19;
  - 313 poz. 1: SW-EA-PF-174/4/19;
  - 397 poz. 5: SW-EA-PF-219/4/19;
  - 645 poz. 2: SW-EA-PF-350/6/19;
  - 662 poz. 2: SW-EA-PF-356/4/19,

  z 2020 roku:
  - 140 poz. 1: PF-146/20;
  - 277 poz. 2: SW-EA-PF-151/6/20;
  - 396 poz. 1: SW-EA-PF-179/4/20; SW-EA-PF-182/4/20;
  - 478 poz. 1: SW-EA-PF-248/11/20; SW-EA-PF-247/11/20;
  - 668 poz. 1: SW-EA-PF-398/11/20,
- funkcjonariusze przetwarzają dokumenty niejawne poza kancelarią zgodnie z przepisami o ochronie informacji niejawnych,
- urządzenia ewidencyjne wykorzystywane w Wydziale II BSWSG prowadzone są zgodnie z zapisami Zarządzenia nr 53 Komendanta Głównego Straży Granicznej z dnia 23 grudnia 2011 r. w sprawie szczegółowego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego,
- obieg dokumentów/materiałów w podmiocie kontrolowanym w większości przypadków odbywa się zgodnie z obowiązującymi przepisami w tym zakresie:

  a) według zapisów w Rejestrze dzienników ewidencji i teczek BSWSG urządzenia ewidencyjne wymienione w:
  - pkt 1 lit. a) do i) były na stanie: [redacted] (zwolnionej ze służby z dniem 11.02.2021r.)
  - pkt 1 lit. j) do m) były na stanie: [redacted] (od dnia 01.03.2019 r. funkcjonariusza Wydziału III BSWSG).

  Powyższe urządzenia ewidencyjne nie zostały przekazane do dalszego prowadzenia innej osobie w Wydziale. W czasie trwania kontroli ww. urządzenia przejął na stan [redacted]

  b) okazane do kontroli dokumenty o numerach: Pf-656/19, zaewidencjonowany w Dzienniku ewidencyjnym korespondencji wchodzącej – poufne (Rdet SW-Z-7/19); Pf-81/20,

zaewidencjonowany w Dzienniku ewidencyjnym korespondencji wchodzącej – poufne (Rdet SW-Z-2/2020); SW-EA-Pf-109/4/DW/20 zaewidencjonowany w Dzienniku ewidencyjnym – dokumenty własne BSWSG (Rdet SW-Z-4/2020), wykorzystywane w podmiocie kontrolowanym były na stanie [redacted] W czasie trwania kontroli ww. dokumenty przejął na stan [redacted]

- sprawdzenie losowo wybranych teczek akt przygotowanych przez Wydział II BSWSG do archiwizacji – nie stwierdzono nieprawidłowości,
- dzienniki ewidencyjne szyfrofaksów wchodzących/wychodzących, prowadzone są w sposób prawidłowy,
- książka rejestracji kart E-15 prowadzone są w sposób prawidłowy,
- nie dokonywano sprawdzeń wpisów w dziennikach rejestracji osób oraz TEO,
- dokumenty wyszczególnione na przekazanych przez Naczelnika Wydziału II BSWSG wykazach dokumentów zostały poddane sprawdzeniu przez zespół kontrolny – stan zgodny.

Ochrona fizyczna realizowana jest w oparciu o:

- Decyzję nr 234 Komendanta Nadwiślańskiego Oddziału Straży Granicznej z dnia 25.09.2019 r. w sprawie wprowadzenia w Komendzie Nadwiślańskiego Oddziału Straży Granicznej *„Planu Ochrony Informacji Niejawnych Komendy Nadwiślańskiego Oddziału Straży Granicznej, w tym w razie prowadzenia stanu nadzwyczajnego"*, z późn. zm. (Dec. nr 210/20 Komendanta NwOSG z dnia 27.11.2020 r.)
- Plan Ochrony Informacji Niejawnych Biura Spraw Wewnętrznych z dnia 28.05.2021 r. (SW-OI.0154.3.2021) oraz Dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą w Biurze Spraw Wewnętrznych Straży Granicznej z dnia 28.05.2021 r. (SW-OI.0154.4.2021).

Sprawdzono i zebrano informacje dotyczące sposobu pobierania i zdawania kluczy (elektroniczny system depozytorów kluczy), zasad wejść i wyjść, przyjmowania interesantów oraz zastosowanych środków bezpieczeństwa określonych w dokumentacji bezpieczeństwa STI w celu potwierdzenia ich zgodności ze stanem faktycznym, tj. numeracja pomieszczeń, wyznaczenie, rozmieszczenie i oznaczenie stref ochronnych, rejestry wejścia/wyjścia do pomieszczeń oraz zabezpieczenia fizyczne – stan faktyczny zgodny z dokumentacją.

Pomieszczenia, w których przetwarzane i przechowywane są dokumenty zawierające informacje niejawne, ujęte są w wykazie pomieszczeń lub obszarów, w których mogą być przetwarzane informacje niejawne. Nie stwierdzono przetwarzania dokumentów niejawnych poza wyznaczonymi do tego pomieszczeniami.

W zakresie bezpieczeństwa teleinformatycznego zespół kontrolny stwierdził:

- zgodność zabezpieczenia akredytowanych stanowisk teleinformatycznych z dokumentacją bezpieczeństwa (okablowanie, prawidłowości podłączenia urządzeń, zabezpieczenie stanowisk plombami, bezpieczeństwo fizyczne), za okres objęty kontrolą,
- zgodność stanu faktycznego informatycznych nośników danych i materiałów wykorzystywanych w systemie ze stanem ewidencyjnym, za okres objęty kontrolą,
- zgodność stanu faktycznego zabezpieczeń globalnego i lokalnego środowiska bezpieczeństwa z dokumentacją bezpieczeństwa,
- zgodność konfiguracji systemu operacyjnego ze stanem faktycznym określonym w dokumentacji bezpieczeństwa, za okres objęty kontrolą,

- zgodność stanu instalacji i konfiguracji oprogramowania antywirusowego oraz aktualność sygnatur baz wirusów, za okres objęty kontrolą,
- zgodność zainstalowanego oprogramowania użytkowego z dokumentacją bezpieczeństwa, za okres objęty kontrolą,
- spełnianie przez użytkowników systemów [redacted] wymagań formalnych do użytkowania stanowisk,
- bieżące prowadzenie i dokumentowanie czynności administracyjnych w „Dzienniku działań administratora".

Na potrzeby czynności kontrolnych sprawdzono następujące wykazy IND zainstalowane w STI Wydziału II BSWSG przeznaczone do przetwarzania informacji niejawnych do klauzuli „poufne" [redacted]) i „tajne" [redacted]

- RWP: SW-EA-Pf-115/19 – dysk twardy zainstalowany w STI [redacted] o identyfikatorze [redacted]
- RWP: SW-EA-Pf-57/19 – dysk twardy zainstalowany w STI [redacted], o identyfikatorze [redacted]
- RWP: SW-EA-0-38/20 – dysk twardy zainstalowany w SUŁ [redacted] o identyfikatorze [redacted]

Dodatkowo zespół kontrolny stwierdził:

- brak wyłączenia konta Inspektora BTI BSWSG [redacted]) w systemie [redacted] odwołanego z funkcji w dniu 18.10.2021 r. Osoba odpowiedzialna: lokalny administrator, Konto wyłączono w tracicie trwania czynności kontrolnych;
- brak wyłączenia konta Inspektora: 015951i na stanowisku systemu [redacted] Konto wyłączono w tracicie trwania czynności kontrolnych;
- brak Zeszytu wydruków próbnych i wadliwych, 41 stron (dokument jawny, RWD 18 SW-1/19) - dokument pobrany przez [redacted] w dniu 30.09.2019 r.

Odnosząc się do skutków stwierdzonych nieprawidłowości należy stwierdzić, że nie doszło do obniżenia poziomu bezpieczeństwa teleinformatycznego w zakresie wdrożonych zabezpieczeń zapewniających poufność, rozliczalność, integralność i dostępność informacji niejawnych. Tym samym nie zachodzą przesłanki do podęcia czynności określonych w art. 17 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2019 poz. 742).

Ocenę sformułowano na podstawie następujących ustaleń:

Stanowisko: [redacted]
Identyfikator: [redacted]
Lokalizacja: budynek Nadwiślańskiego OSG nr 2, piętro II, pom. nr 218
Sprzęt: All In One: ThinkCentre Lenovo, sn: PC16Q8KP,
klawiatura: Lenovo przewodowa sn: 0101209,
mysz: Lenovo przewodowa, optyczna, sn: 8SSM50L24505AVLC96C0CM3,
HDD/SSD: Samsung, sn: 0025-3886-91B8-DBCD,
drukarka: Konica Minolta bizhub 4000P, sn: A63R021173677,
numery seryjne zgodne z dokumentacją bezpieczeństwa.
Plomby: obudowa: BOIN KGSG nr 0742, 0743.

Dokumentacja:

- Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego nr 201/2021 z dnia 27.09.2021 r. dla stanowiska dostępowego [redacted] ważne do dnia 30.06.2026 r.;
- Szczególne Wymagania Bezpieczeństwa Systemu Teleinformatycznego Centralna Baza Danych [redacted] KG-OI-Z-562/21;
- Procedury Bezpiecznej Eksploatacji Systemu Teleinformatycznego Centralna Baza Danych [redacted] KG-OI-Z-563/21;
- Procedury Bezpiecznej Eksploatacji Systemu Teleinformatycznego Centralna Baza Danych [redacted] – procedura konfiguracji systemu Microsoft Windosw 10 Enterprise [redacted] (dla stanowisk o klauzuli poufne), KG-OI-Z-567/21;
- Opis stanowiska dostępowego Systemu [redacted] zlokalizowanego w Biurze Spraw Wewnętrznych Straży Granicznej z siedzibą w budynku Komendy Nadwiślańskiego OSG, ul. Komitetu Obrony Robotników 23, 02-148 Warszawa, którego jednostką organizującą system jest Komenda Główna Straży Granicznej (SW-OI-Z-610/11/DW/21);
- Rejestr wejść i wyjść do pomieszczenia nr 218 i 217; RWD 47/poz. 4/2020, rozpoczęto w dniu 09.11.2020 r., na dzień 23.05.2022 r., ostatni wpis na poz. 166;
- Zeszyt wydruków próbnych i wadliwych systemu [redacted]; RWD 47-SW-4/19, rozpoczęto w dniu 10.01.2020 r., na dzień 23.05.2022 r., brak wpisów poz.;
- Dziennik działań administratora Systemu [redacted], RWD 67-SW-OI-2/21, rozpoczęto w dniu 26.04.2021r., na dzień 23.05.2022r., ostatni wpis na poz. 129.

Lp.	Zakres kontroli	Miernik kontroli	Ocena kontrolowanego zagadnienia	Uwagi
1	prawidłowość podłączenia do sieci teleinformatycznej	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
2	terminowy przegląd okablowania przez lokalnego administratora	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
3	zabezpieczenie stanowisk plombami	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
4	rejestracja informatycznych nośników danych i materiałów wykorzystywanych w systemie	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
5	prawidłowość konfiguracji ustawień BIOS	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
6	prawidłowość konfiguracji wybranych elementów systemu operacyjnego	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-

7	instalacja i konfiguracja oprogramowania antywirusowego	zainstalowane oprogramowanie antywirusowe oraz poprawna jego konfiguracja	pozytywna	-
8	aktualność oprogramowania antywirusowego	termin aktualizacji zgodny z dokumentacją bezpieczeństwa	pozytywna	-
9	zgodność zainstalowanego oprogramowania użytkowego z dokumentacją bezpieczeństwa	**80% – 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
10	zakładanie i usuwanie kont na podstawie zleceń nadania/cofnięcia uprawnień	**90% - 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
11	zabezpieczenia fizyczne	**90% - 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
12	wyznaczanie 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	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
13	posiadanie przez lokalnego administratora podpisanych oświadczeń przez użytkowników systemu o zapoznaniu się z PBE	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
14	prowadzenie „dziennika działań administratora" przez lokalnego administratora	**do 2** brakujących wpisów potwierdzających fakt wykonania prac administracyjnych lub związanych z bezpieczeństwem stanowiska	pozytywna	-
15	przeprowadzenie analizy i archiwizacji logów systemowych przez lokalnego administratora	**80% - 100%** wpisów potwierdzających fakt dokonania analizy i archiwizacji logów systemowych	pozytywna	-
16	aktualizacja opisów stanowisk	suma błędnych lub nieaktualnych wpisów **mniejsza lub równa 5**	pozytywna	-
17	posiadanie przez lokalnego administratora niezbędnej dokumentacji bezpieczeństwa oraz dokumentacji pomocniczej	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-

Stanowisko: [redacted]
Identyfikator: [redacted]
Lokalizacja: budynek Nadwiślańskiego OSG nr 2, piętro II, pom. nr 217
Sprzęt: All In One: ThinkCentre Lenovo, sn: PC01D01S
monitor:-
klawiatura: Lenovo przewodowa sn:0017616,

mysz: Lenowo przewodowa, optyczna, sn: 4440540,
HDD/SSD: Samsung, sn: W3TJXQ03,
drukarka: -
skaner:-
numery seryjne zgodne z dokumentacją bezpieczeństwa
Plomby: obudowa: BOIN KGSG 0786.

Dokumentacja:

- Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego nr 193/2021 z dnia 27.09.2021 r. dla stanowiska dostępowego [redacted], ważne do dnia 31.05.2026 r.;
- Szczególne Wymagania Bezpieczeństwa, Lj-Z-261/2021;
- Opis stanowiska dostępowego Systemu [redacted] zlokalizowanego w Biurze Spraw Wewnętrznych Straży Granicznej w Warszawie, którego, którego jednostką organizującą system jest Komenda Główna Policji, (SW-OI-Z 649/8/DM/21);
- Karta zapoznania się z dokumentacją bezpieczeństwa [redacted], (RWD 59-SW-OI-1/21);
- Dziennik działań Administratora Bezpieczeństwa Teleinformatycznego [redacted], (RWD 59-SW-OI-3/21);
- Zeszyt wydruków próbnych i wadliwych Systemu Niejawnego Policji [redacted], (RWD 47-SW-OI-2/21);
- Rejestr wejść i wyjść do pomieszczenia nr 218 i 217; RWD 47/poz. 4/2020, rozpoczęto w dniu 09.11.2020 r., na dzień 23.05.2022 r., ostatni wpis na poz. 166.

Lp.	Zakres kontroli	Miernik kontroli	Ocena kontrolowanego zagadnienia	Uwagi
1	prawidłowość podłączenia do sieci teleinformatycznej	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
2	terminowy przegląd okablowania przez lokalnego administratora	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
3	zabezpieczenie stanowisk plombami	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
4	rejestracja informatycznych nośników danych i materiałów wykorzystywanych w systemie	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
5	prawidłowość konfiguracji ustawień BIOS	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
6	prawidłowość konfiguracji wybranych elementów systemu operacyjnego	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
7	instalacja i konfiguracja oprogramowania antywirusowego	zainstalowane oprogramowanie antywirusowe oraz poprawna jego konfiguracja	pozytywna	-
8	aktualność oprogramowania antywirusowego	termin aktualizacji zgodny z dokumentacją bezpieczeństwa	pozytywna	-

9	zgodność zainstalowanego oprogramowania użytkowego z dokumentacją bezpieczeństwa	**80% – 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
10	zakładanie i usuwanie kont na podstawie zleceń nadania/cofnięcia uprawnień	**90% - 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
11	zabezpieczenia fizyczne	**90% - 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
12	wyznaczanie 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	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
13	posiadanie przez lokalnego administratora podpisanych oświadczeń przez użytkowników systemu o zapoznaniu się z PBE	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-
14	prowadzenie „dziennika działań administratora" przez lokalnego administratora	**do 2** brakujących wpisów potwierdzających fakt wykonania prac administracyjnych lub związanych z bezpieczeństwem stanowiska	pozytywna	-
15	przeprowadzenie analizy i archiwizacji logów systemowych przez lokalnego administratora	**80% - 100%** wpisów potwierdzających fakt dokonania analizy i archiwizacji logów systemowych	pozytywna	-
16	aktualizacja opisów stanowisk	suma błędnych lub nieaktualnych wpisów **mniejsza lub równa 5**	pozytywna	-
17	posiadanie przez lokalnego administratora niezbędnej dokumentacji bezpieczeństwa oraz dokumentacji pomocniczej	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	-

Stanowisko: [redacted]
Identyfikator: [redacted]
Lokalizacja: budynek Nadwiślańskiego OSG nr 2, piętro II, pom. nr 217
Sprzęt: [redacted]: szyfrator transmisji telekopiowej: [redacted]
[redacted]n:AK49040941.
[redacted] szyfrator transmisji telekopiowej: [redacted]
[redacted] sn:AK49040860.
[redacted] Konica Minolta bizhub C3851 [redacted] A92E021005754.

numery seryjne zgodne z dokumentacją bezpieczeństwa.

Plomby: stanowiska zabezpieczone plombami ABW.

Dokumentacja:

[redacted]

- Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego nr 31/2021, ważne do dnia 30.06.2023 r.
- Szczególne Wymagania Bezpieczeństwa (KG-OI-Z-204/20);
- Procedury Bezpiecznej Eksploatacji (KG-OI-Z-203/20);
- Rejestr Operatorów stanowiska [redacted] w Warszawie;
- Karta zapoznania się z dokumentacją bezpieczeństwa [redacted];
- Opis stanowiska dostępowego [redacted] (SW-OI-Z-78/9/DW/21);
- Dziennik działań lokalnego administratora systemu (RWD 59-SW-OI-1/20).

[redacted]

- Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego nr 54/2021, ważne do dnia 31.05.2023 r.;
- Szczególne Wymagania Bezpieczeństwa (N-Pf-14529/2020);
- Procedury Bezpiecznej Eksploatacji (N-Pf-14514/2020);
- Opis stanowiska dostępowego [redacted] (SW-OI-Z-76/9/DW/21);
- Dziennik pracy lokalnego Administratora [redacted] SW-OI-Z-274/8/DW/20);
- Karta zapoznania się z dokumentacją bezpieczeństwa [redacted] (bez numeru);
- Wykaz operatorów [redacted] (bez numeru).

[redacted]

- Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego nr 53/2021, ważne do dnia 31.05.2023 r.;
- Wyciąg ze Szczególnych Wymagań Bezpieczeństwa (N-Pf-33462/2018);
- Wyciąg ze Szczególnych Wymagań Bezpieczeństwa (N-Pf-33474/2018) wraz z aneksem nr 1 do PBE (N-Z-4531/2019),
- Instrukcja Administratora Lokalnego Aplikacja [redacted] wersja 2.0, (SW-OI-Z-176/9/DW/20),
- Instrukcja Inspektora BTI Aplikacja [redacted], wersja 2.0, (SW-OI-Z-178/9/DW/20),
- Opis stanowiska dostępowego systemu utajnionej łączności kryptonim [redacted] (SW-OI-Z-80/9/DW/21),
- Dziennik pracy lokalnego Administratora [redacted] (SW-OI-Z-265/8/DW/20).
- Karta zapoznania się z dokumentacją bezpieczeństwa [redacted]

Lp.	Zakres kontroli	Miernik kontroli	Ocena kontrolowanego zagadnienia	Uwagi
1	prawidłowość podłączenia do sieci teleinformatycznej	100% zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]

2	terminowy przegląd okablowania przez lokalnego administratora	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]
3	zabezpieczenie stanowisk plombami	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]
4	rejestracja informatycznych nośników danych i materiałów wykorzystywanych w systemie	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]
5	prawidłowość konfiguracji ustawień BIOS	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	-	Nie dotyczy
6	prawidłowość konfiguracji wybranych elementów systemu operacyjnego	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	-	Nie dotyczy
7	instalacja i konfiguracja oprogramowania antywirusowego	zainstalowane oprogramowanie antywirusowe oraz poprawna jego konfiguracja	-	Nie dotyczy
8	aktualność oprogramowania antywirusowego	termin aktualizacji zgodny z dokumentacją bezpieczeństwa	-	Nie dotyczy
9	zgodność zainstalowanego oprogramowania użytkowego z dokumentacją bezpieczeństwa	**80% – 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	-	Nie dotyczy
10	zakładanie i usuwanie kont na podstawie zleceń nadania/cofnięcia uprawnień	**90% - 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]
11	zabezpieczenia fizyczne	**90% - 100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]
12	wyznaczanie 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	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]
13	posiadanie przez lokalnego administratora podpisanych oświadczeń przez użytkowników systemu o zapoznaniu się z PBE	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]
14	prowadzenie „dziennika działań administratora" przez lokalnego administratora	**do 2** brakujących wpisów potwierdzających fakt wykonania prac administracyjnych lub związanych z bezpieczeństwem stanowiska	pozytywna	dotyczy: [redacted]

15	przeprowadzenie analizy i archiwizacji logów systemowych przez lokalnego administratora	**80% - 100%** wpisów potwierdzających fakt dokonania analizy i archiwizacji logów systemowych	-	Nie dotyczy
16	aktualizacja opisów stanowisk	suma błędnych lub nieaktualnych wpisów **mniejsza lub równa 5**	pozytywna	[redacted]
17	posiadanie przez lokalnego administratora niezbędnej dokumentacji bezpieczeństwa oraz dokumentacji pomocniczej	**100%** zgodności stanu faktycznego z dokumentacją bezpieczeństwa	pozytywna	dotyczy: [redacted]

VII. Wnioski i zalecenia dotyczące usprawnienia funkcjonowania podmiotu kontrolowanego.

W związku z uzyskaną oceną końcową kontroli pozytywną, nie formułowano wniosków i zaleceń.
Jednocześnie w dniu 28.06.2022 r. okazano Zeszyt wydruków próbnych i wadliwych, 41 stron (dokument jawny, RWD 18 SW-1/19), który nie był przedstawiony do kontroli w okresie przeprowadzania czynności kontrolnych.

VIII. Zgodnie z § 34 wytycznych stanowiących załącznik 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. Min. Spraw Wew. poz. 43, z późn. zm.) od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

IX. Fakt przeprowadzenia kontroli w trybie zwykłym, odnotowano w Książce kontroli Wydziału Ochrony Informacji Biura Spraw Wewnętrznych Straży Granicznej (Rdet SW-14/19), pozycja nr 1/2022.

X. Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach, z których egzemplarz nr 1 jest przeznaczony dla kierownika podmiotu kontrolowanego.

KOMENDANT
BIURA SPRAW WEWNĘTRZNYCH
STRAŻY GRANICZNEJ

płk SG Adam WANARSKI

.....

(stopień, imię i nazwisko oraz podpis zarządzającego kontrolę

Wykonano w 2 egzemplarzach
dnia 28.06.2022 r.
Egz. nr 1 – Naczelnik Wydziału II BSWSG
Egz. nr 2 – ad acta.
Wykonał: Zespół kontrolny [redacted]