**Uzgodniono**

PLAN AKREDYTACJI

SYSTEMU TELEINFORMATYCZNEGO

**NAZWA SYSTEMU**

Wersja 1.0

**Opracował:**

(podpis organizatora systemu)

**INFORMACJE WSTĘPNE**

Przedmiotowy dokument stanowi wzór planu akredytacji, jaki na etapie projektowania systemu zobowiązany jest opracować organizator systemu.

Wytyczne do opracowania przedmiotowego dokumentu:

1. Dokument opracowuje w jednym egzemplarzu jednostka/komórka organizacyjna resortu obrony narodowej pełniąca funkcję Organizatora Systemu.
2. W sytuacji gdy Organizator Systemu podejmuje decyzję o pominięciu etapu planowania oraz projektowania i przystępuje do opracowania dokumentacji bezpieczeństwa (tj. SWB i PBE) co jest czynnością właściwą do realizacji
na etapie wdrażania, niniejszego dokumentu nie opracowuje się.
3. Klauzulę dokumentu określa jego wykonawca.
4. W przypadku konieczności zmiany zapisów uzgodnionego poprzednio z SKW planu akredytacji, Organizator Systemu nie sporządza do niego aneksu,
tylko opracowuje kolejną jego wersję.
5. W niniejszym wzorze tekst koloru czarnego jest tekstem obligatoryjnym,
który nie powinien być zmieniany.
6. W niniejszym wzorze tekst oznaczony kolorem czerwonym podlega edycji przez opracowującego dokument stosownie do opisywanego systemu teleinformatycznego.
7. W niniejszym wzorze tekst oznaczony kolorem niebieskim należy z docelowego dokumentu usunąć – stanowi on jedynie wskazówki
i informacje, co powinny zawierać poszczególne rozdziały lub dodatkowe komentarze i wyjaśnienia.

Z docelowego dokumentu przedmiotową stronę należy usunąć.

**STRONA KONTROLI DOKUMENTU**

|  |  |  |
| --- | --- | --- |
| Wersja | Data | Przyczyna zmiany[[1]](#footnote-1) |
| 1.0 | ….. | Pierwotna wersja dokumentu |
|  |  |  |
|  |  |  |

Spis treści

[I. Cel akredytacji 5](#_Toc87610209)

[II. Dane kontaktowe 5](#_Toc87610210)

[II.1. Organizator Systemu 5](#_Toc87610211)

[II.2. Przedstawiciel Organizatora Systemu – kierownik projektu wdrożenia systemu 6](#_Toc87610212)

[II.3. Przedstawiciel SKW odpowiedzialny za prowadzenie procesu akredytacji
 bezpieczeństwa teleinformatycznego systemu 6](#_Toc87610213)

[III. Dokumenty odniesienia 7](#_Toc87610214)

[IV. Opis systemu 7](#_Toc87610238)

[IV.1. Przeznaczenie Systemu 7](#_Toc87610239)

[V. Personel bezpieczeństwa biorący udział w procesie akredytacji i jego zadania 7](#_Toc87610249)

[VI. Zakres i harmonogram działań zmierzających do uzyskania akredytacji 9](#_Toc87610426)

**Spis diagramów i tabel**

[Tabela V.1. Personel bezpieczeństwa występujący w planowanym systemie 8](#_Toc87606317)

[Tabela VI.1. Harmonogram 9](#_Toc87606318)

**Przedmiotowy dokument stanowi plan akredytacji systemu teleinformatycznego NAZWA SYSTEMU opracowanego w celu wypełnienia wymagań określonych §18 ust. 3 pkt 3 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948).**

# Cel akredytacji

SKW udziela albo odmawia udzielenia akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej.

1. Zgodnie z art. 2 ust. 10 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756), zwanej dalej „ustawą”, akredytacja bezpieczeństwa teleinformatycznego (ABT) to dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych.

Zgodnie z art. 48 ust. 3 ustawy SKW udziela albo odmawia udzielenia ABT
dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej po potwierdzeniu, że w systemie teleinformatycznym zaimplementowano mechanizmy bezpieczeństwa wymagane zgodnie z obowiązującymi przepisami.

Potwierdzeniem udzielenia ABT jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego, które zgodnie z art. 48 ust. 6 ustawy wystawiane jest na podstawie:

1. zatwierdzonej dokumentacji bezpieczeństwa systemu teleinformatycznego;
2. wyników audytu bezpieczeństwa systemu teleinformatycznego.

# Dane kontaktowe

### Organizator Systemu

Nazwa jednostki organizacyjnej:

Adres:

Kierownik JO:

### Przedstawiciel Organizatora Systemu – kierownik projektu wdrożenia systemu

* 1. ……………..:
* poświadczenie bezpieczeństwa nr ………..;
* tel.: …………;
* tel. komórkowy…………
	1. ………………:
* poświadczenie bezpieczeństwa nr ………...;
* tel.: …………;
* tel. komórkowy…………

### Przedstawiciel SKW odpowiedzialny za prowadzenie procesu akredytacji bezpieczeństwa teleinformatycznego systemu

*(dane kontaktowe osoby odpowiedzialnej za prowadzenie procesu ABT systemu zostaną uzupełnione przez SKW na etapie uzgadniania przedmiotowego dokumentu)*

Stopień, imię i nazwisko:…………………………………………………

tel.:………………………………………………………………………….

tel. komórkowy:……………………………………………………………

E- mail:……………………………………………………………...……..

# Dokumenty odniesienia

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756).
2. Rozporządzenie Prezesa Rady Ministrów z 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r.
Nr 159, poz. 948).

Jeżeli to konieczne można zawrzeć inne akty i dokumentu normatywne, które bezpośrednio będą mieć wpływ na ochronę informacji niejawnych w organizowanym systemie teleinformatycznym.

# Opis systemu

Należy zawrzeć krótki opis organizowanego systemu teleinformatycznego ze szczególnym uwzględnieniem mechanizmów, zabezpieczeń oraz technologii wykorzystywanych w jego budowie do zapewnienia poufności, integralności i dostępności informacji niejawnych. W niniejszym punkcie można także dla dokładniejszego opisu systemu zawierać elementy graficzne zawierające planowaną architekturę systemu lub konkretnych rozwiązań technicznych zapewniających bezpieczeństwa informacji niejawnych. Dla systemów teleinformatycznych, w których planowane jest wykorzystywania połączeń międzysystemowych dodatkowo należy w formie tekstowej lub graficznej zdefiniować granicę akredytacji systemu teleinformatycznego, w tym opisać wykorzystywane interfejsy oraz przepływ danych.

### Przeznaczenie Systemu

Należy zawrzeć opis przeznaczenia systemu teleinformatycznego ze szczególnym jego uwzględnieniem jego rozległości, charakteru wykorzystania lub wymagań operacyjnych stawianych przed przedmiotowym systemem.

# Personel bezpieczeństwa biorący udział w procesie akredytacji i jego zadania

W niniejszym punkcie w formie tabelarycznej należy przedstawić planowane w systemie role/osoby funkcyjne/personel bezpieczeństwa wraz z ich zadaniami. Zawarta poniżej przykładowa tabela zawiera niezbędne osoby funkcyjne/personel bezpieczeństwa, które powinny być powołane w każdym systemie teleinformatycznym w celu uzyskania ABT. Przedmiotową tabelę Organizator Systemu można dowolnie uzupełniać o role/osoby funkcyjne/personel bezpieczeństwa w zależności od charakteru organizowanego systemu teleinformatycznego.

Tabela V.1. Personel bezpieczeństwa występujący w planowanym systemie

| Rola/personel bezpieczeństwa | Opis | Wymagania |
| --- | --- | --- |
| Organizator Systemu | odpowiedzialność została określona w art. 14 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756). |  |
| Pełnomocnik ds. Ochrony Informacji Niejawnych | odpowiedzialność została określona w art. 14 ust. 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756). |  |
| Oficer Bezpieczeństwa Systemów Łączności i Informatyki[[2]](#footnote-2) | odpowiedzialność została określona w §7 pkt 12 Zarządzenia nr 46/MON Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz.Urz.MON z 2013 r. poz 401 z późn. zm.) oraz w pkt. 6 załącznika nr 1 do Decyzji nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 r. w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej (Dz. Urz. MON z 2012 r. poz. 8). |  |
| Administrator Systemu  | odpowiedzialność została określona w art. 52 ust. 1 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756). |  |
| Inspektor Bezpieczeństwa Teleinformatycznego | odpowiedzialność została określona w art. 52 ust. 1 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756). |  |

# Zakres i harmonogram działań zmierzających do uzyskania akredytacji

W niniejszym punkcie w formie tabelarycznej należy przedstawić niezbędne czynności, które zamierza podjąć Organizator Systemu w celu uzyskania ABT. Zawarta poniżej przykładowa tabela zawiera obligatoryjne czynności, które będą musiały być przeprowadzone podczas procesu ABT dla każdego systemu teleinformatycznego. Przedmiotową tabelę Organizator Systemu można dowolnie uzupełniać o dodatkowe czynności w każdym etapie cyklu życia systemu teleinformatycznego, które w jego ocenie są istotne lub wręcz niezbędne
do uzyskania świadectwa bezpieczeństwa systemu teleinformatycznego, przy czym za realizację przedmiotowych dodatkowych czynności nie może być odpowiedzialny organ udzielający akredytacji.

Tabela VI.1. Harmonogram

| Zagadnienie | Odpowiedzialny | Status | Planowana data rozpoczęcia | Planowana datazakończenia | Uwagi |
| --- | --- | --- | --- | --- | --- |
| **1.0 Etap planowania** |  |
|  | ………… | powołana rola/osoba funkcyjna/ personel bezpieczeństwa | **Wykonane lub Niezrealizowano** |  |  |  |
|  | Określenie Technicznego Poziomu Zabezpieczenia Urządzenia lub klasy urządzenia w ramach certyfikacji zgodnie z art. 50 ust. 1 i 4 ustawy[[3]](#footnote-3), a także osobne konsultacje z SKW[[4]](#footnote-4). | Organizator Systemu/Zarząd VI SKW | **W trakcie** | Zgodnie z oddzielnym harmonogramem |
| **2.0 Etap projektowania**  |  |
|  | Uzgodnienie planu akredytacji |  Zarząd VI SKW | **W trakcie** |  |  |  |
| **3.0 Etap wdrażenia** |  |
|  | Uzgodnienie dokumentacji bezpieczeństwa zgodnie z Decyzją Nr 62/DK WOC Ministra Obrony Narodowej z dnia 14 marca 2023 r. w sprawie organizacji i funkcjonowania systemu cyberbezpieczeństwa w resorcie obrony narodowej (niepublikowana)[[5]](#footnote-5) | Organizator Systemu/DKWOC | **W trakcie** |  |  |  |
|  | Przesłanie kompletnej dokumentacji bezpieczeństwa do Zarządu VI SKW | Organizator Systemu | **W trakcie** |  |  |  |
|  | Zatwierdzenie dokumentacji bezpieczeństwa | Zarząd VI SKW | **W trakcie** |  |  |  |
|  | Przygotowanie i zgłoszenie systemu do audytu bezpieczeństwa systemu teleinformatycznego | Organizator Systemu | **W trakcie** |  |  |  |
|  | Audyt bezpieczeństwa systemu teleinformatycznego | Zarząd VI SKW | **W trakcie** |  |  |  |
|  | Udzielenie akredytacji i wydanie dokumentu akredytacyjnego | Zarząd VI SKW | **W trakcie** |  |  |  |

Wykonano w egz. pojedynczym

Wykonał:…

1. Po każdorazowym opracowywaniu nowej wersji dokumentu należy zamieścić w tabeli podstawę jej opracowywania. Może to być rozkaż/decyzja kierownika JO/KO, pismo/protokół/notatka związane z uruchomianiem systemu mające wpływ na jego akredytację lub zalecenia SKW. Tabela powinna zawierać informację o wszystkich wersjach przedmiotowego dokumentu, które zostały uzgodnione uprzednio z SKW (nie numery wersji roboczych dokumentu opracowywanego wewnętrznie w JO/KO). [↑](#footnote-ref-1)
2. tylko dla systemów niejawnych, w których stosowane są urządzenia lub narzędzia kryptograficzne
lub przetwarzających materiały kryptograficzne. [↑](#footnote-ref-2)
3. przedmiotowa czynność może być także wykonana w innym etapie cyklu życia, przy czym musi być zakończona przed zgłoszeniem systemu teleinformatycznego do audytu bezpieczeństwa teleinformatycznego. [↑](#footnote-ref-3)
4. konsultacja z SKW jest wymagana w przypadkach opisanych w tabeli nr 5 zawartej w Zaleceniach ogólnych Służby Kontrwywiadu Wojskowego w zakresie zapewnienia ochrony elektromagnetycznej systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych ZOBT-500A. [↑](#footnote-ref-4)
5. przedmiotowa czynność jest wymagana tylko dla rozległych systemów teleinformatycznych przetwarzających informacje niejawne zgodnie z §13 ust. 2) oraz załącznikiem nr 3 do Decyzji Nr 62/DK WOC Ministra Obrony Narodowej z dnia 14 marca 2023 r. w sprawie organizacji
i funkcjonowania systemu cyberbezpieczeństwa w resorcie obrony narodowej (niepublikowana). [↑](#footnote-ref-5)