**AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO**

**DEPARTAMENT BEZPIECZEŃSTWA TELEINFORMATYCZNEGO**

**WNIOSEK WA-01**

**o przeprowadzenie audytu bezpieczeństwa systemu teleinformatycznego oraz wydanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego**

**Wniosek WA-01 wypełnia się po zatwierdzeniu przez Agencję Bezpieczeństwa Wewnętrznego w trybie art. 49 ust. 8 UOIN dokumentacji bezpieczeństwa systemu teleinformatycznego lub/i aneksu zawierającego dane dotyczące konkretnej lokalizacji, sporządzonego przez kierownika jednostki organizacyjnej, w której znajdują się elementy systemu TI (§ 27 RPRM BTI).**

**Wypełnienie i przesłanie do ABW wniosku WA-01 oznacza pełną gotowość wnioskodawcy do wykonania czynności audytowych przez ABW.**

1. **Wniosek WA dotyczy przeprowadzenia audytu dla:**

|  |
| --- |
| [ ]  Autonomicznego stanowiska/stanowisk systemu teleinformatycznego (ASTI) „     ” |
| LAN/WAN systemu teleinformatycznego „     ” |
| [ ]  Centralnego węzła/serwerowni systemu TI „     ” |
| [ ]  Lokalnego węzła systemu TI „     ” |
| [ ]  Stanowiska/stanowisk dostępowych systemu teleinformatycznego „     ” |
| [ ]  Innego (jakiego):       |

1. **Zgłoszenie:**

|  |  |  |
| --- | --- | --- |
| [ ]  Pierwszy raz | [ ]  Ponowna akredytacja | [ ]  Po dokonanych zmianach w STI |

1. **Maksymalna klauzula informacji niejawnych przetwarzanych w STI:**

|  |  |  |  |
| --- | --- | --- | --- |
| **KRAJOWE:** |  | **UE:** |  |
| **NATO:** |  | **ESA:** |  |
| **INNE:** |       |

1. **Dokumentacja bezpieczeństwa systemu TI tj.: Szczególne Wymagania Bezpieczeństwa i Procedury Bezpiecznej Eksploatacji:**

|  |  |
| --- | --- |
| Sygnatura literowo-cyfrowa dokumentu SWB:  |       |
| Sygnatura literowo-cyfrowa dokumentu PBE:  |       |
| Sygnatura literowo-cyfrowa pisma ABW zatwierdzającego wyżej wymienioną dokumentację:  | Nr:       z dnia:       |

1. **Należy wypełnić w przypadku, gdy wniosek dotyczy przeprowadzenia audytu elementów systemu TI
(§ 27 RPRM BTI) np. stanowisk dostępowych systemu teleinformatycznego:**

|  |  |
| --- | --- |
| Sygnatura literowo-cyfrowa dokumentu opisującego elementy systemu TI:  |       |
| Sygnatura literowo-cyfrowa pisma ABW zatwierdzającego wyżej wymieniony opis elementów systemu TI:  | Nr:       z dnia:       |

1. **Należy wypełnić w przypadku, gdy wniosek dotyczy przeprowadzenia audytu dla wprowadzanych zmian na podstawie aneksów w systemie TI posiadającym akredytację bezpieczeństwa teleinformatycznego:**

|  |  |
| --- | --- |
| Sygnatura literowo-cyfrowa aneksu dokumentu SWB:  |       |
| Sygnatura literowo-cyfrowa aneksu dokumentu PBE:  |       |
| Sygnatura literowo-cyfrowa pisma ABW zatwierdzającego wyżej wymienione aneksy:  | Nr:       z dnia:       |

1. **Dane jednostki organizacyjnej organizującej / użytkującej system TI i przeznaczenie systemu TI:**

|  |  |
| --- | --- |
| * 1. Nazwa i adres jednostki organizacyjnej organizującej system
 | Nazwa JO:      ul.       miejscowość:      kod:       |
| * 1. Nazwa i adres jednostki organizacyjnej, w której będą funkcjonowały elementy systemu TI
 | Nazwa JO:      ul.      miejscowość:      kod:       |
| * 1. Lokalizacja elementów systemu TI (adres, piętro, nr pomieszczenia, dane identyfikacyjne stanowiska np. numer/nazwa stanowiska)
 | Nazwa JO:      ul.      miejscowość:      kod:      budynek:      piętro:      nr pomieszczenia:      [ ]  strefa ochronna I,[ ]  strefa ochronna II[ ]  strefa ochronna IIIIdentyfikator/nazwa/numer stanowiska[[1]](#footnote-1):        |
| * 1. Rodzaj jednostki organizacyjnej
 | [ ]  jednostka organizacyjna podlegająca opłatom, o których mowa w art. 53 ust. 1 UOIN, za czynności akredytacyjne, o których mowa w art. 48 ust. 3-6 UOIN |
| [ ]  jednostka budżetowa, w rozumieniu art. 11 ustawy z dnia 27 sierpnia2009 r. o finansach publicznych |
| [ ]  przedsiębiorca obowiązany na podstawie odrębnych przepisów do wykonywania zadań publicznych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego Nr decyzji administracyjnej:      Nr umowy:       |
| * 1. Przeznaczenie systemu

teleinformatycznego[[2]](#footnote-2) | [ ]  system teleinformatyczny organizowany jest w celu wykonywania przez wnioskodawcę zadań publicznych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, do których realizacji przedsiębiorca jest obowiązany na podstawie odrębnych przepisów, (zgodnie z art. 53 ust. 3 UOIN) |
| [ ]  realizacja innych zadań, niż określone w art. 53 ust. 3 UOIN |

1. **Dane identyfikacyjne wnioskodawcy:**

|  |  |  |
| --- | --- | --- |
| NIP wnioskodawcy: | REGON wnioskodawcy: | KRS wnioskodawcy: |
|       |       |       |

1. **Kierownik jednostki organizacyjnej (w rozumieniu UOIN), w której będzie funkcjonował
system TI / elementy systemu TI (§ 27 RPRM BTI):**

|  |  |
| --- | --- |
| Stanowisko:  |       |
| Imię i nazwisko:  |       |
| Telefon:  |       |
| **Poświadczenia bezpieczeństwa** |
|  | Nr poświadczenia bezpieczeństwa | Klauzula | Data wydania |
| Krajowe  |       |  |       |
| NATO |       |  |       |
| UE  |       |  |       |
| ESA  |       |  |       |
| INNE  |       |       |       |
| **Przeszkolenie z zakresu ochrony informacji niejawnych**  |
|  | Nr zaświadczenia | Data szkolenia |
| Krajowe  |       |       |
| NATO  |       |       |
| UE  |       |       |
| ESA  |       |       |
| INNE  |       |       |

1. **Pełnomocnik ds. ochrony informacji niejawnych w jednostce organizacyjnej, w której będzie funkcjonował system TI / elementy systemu TI (§ 27 RPRM BTI):**

|  |  |
| --- | --- |
| Imię i nazwisko:  |       |
| Telefon:  |       |
| Nr dokumentu, na podstawie którego został wyznaczony Pełnomocnik ds. ochrony informacji niejawnych |       |
| **Poświadczenia bezpieczeństwa** |
|  | Nr poświadczenia bezpieczeństwa | Klauzula | Data wydania |
| Krajowe  |       |  |       |
| NATO  |       |  |       |
| UE  |       |  |       |
| ESA  |       |  |       |
| INNE  |       |       |       |
| **Przeszkolenie z zakresu ochrony informacji niejawnych**  |
|  | Nr zaświadczenia | Data szkolenia |
| Krajowe  |       |       |
| NATO  |       |       |
| UE  |       |       |
| ESA  |       |       |
| INNE  |       |       |

1. **Inspektor/Inspektorzy bezpieczeństwa teleinformatycznego w jednostce organizacyjnej,
w której będzie funkcjonował system TI / elementy systemu TI (§ 27 RPRM BTI), wyznaczeni przez kierownika jednostki organizacyjnej zgodnie z art. 52 ust. 1 pkt 1 UOIN:**

|  |  |
| --- | --- |
| Imię i nazwisko:  |       |
| Telefon:  |       |
| Nr dokumentu, na podstawie którego został wyznaczony inspektor BTI |       |
| Osoba wyznaczająca inspektora BTI |       |
| **Poświadczenia bezpieczeństwa** |
|  | Nr poświadczenia bezpieczeństwa | Klauzula | Data wydania |
| Krajowe  |       |  |       |
| NATO  |       |  |       |
| UE  |       |  |       |
| ESA  |       |  |       |
| INNE  |       |       |       |
| **Przeszkolenie z zakresu ochrony informacji niejawnych**  |
|  | Nr zaświadczenia | Data szkolenia |
| Krajowe  |       |       |
| NATO  |       |       |
| UE  |       |       |
| ESA  |       |       |
| INNE  |       |       |
| Nr zaświadczenia o odbyciu specjalistycznego szkolenia prowadzonego przez ABW lub SKW w trybie art. 52 ust. 4 UOIN |       |

1. **Administrator/Administratorzy systemu w jednostce organizacyjnej, w której będzie funkcjonował system TI / elementy systemu TI (§ 27 RPRM BTI), wyznaczeni przez kierownika jednostki organizacyjnej zgodnie z art. 52 ust. 1 pkt. 2 UOIN:**

|  |  |
| --- | --- |
| Imię i nazwisko:  |       |
| Telefon:  |       |
| Nr dokumentu, na podstawie którego został wyznaczony administrator systemu |       |
| Osoba wyznaczająca administratora systemu |       |
| **Poświadczenia bezpieczeństwa** |
|  | Nr poświadczenia bezpieczeństwa | Klauzula | Data wydania |
| Krajowe |       |  |       |
| NATO  |       |  |       |
| UE  |       |  |       |
| ESA  |       |  |       |
| INNE  |       |       |       |
| **Przeszkolenie z zakresu ochrony informacji niejawnych**  |
|  | Nr zaświadczenia | Data szkolenia |
| Krajowe |       |       |
| NATO  |       |       |
| UE  |       |       |
| ESA  |       |       |
| INNE  |       |       |
| Nr zaświadczenia o odbyciu specjalistycznego szkolenia prowadzonego przez ABW lub SKW w trybie art. 52 ust. 4 UOIN |       |

1. **Bezpieczeństwo osobowe:**

|  |  |  |
| --- | --- | --- |
| * 1. Wszystkie osoby odpowiedzialne za bezpieczeństwo systemu TI (AS/IBTI) zostały formalnie wyznaczone przez kierownika jednostki organizacyjnej
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wszyscy użytkownicy posiadają poświadczenia bezpieczeństwa lub inne stosowne uprawnienia do dostępu do informacji niejawnych, adekwatne do klauzuli informacji niejawnych przetwarzanych w systemie oraz trybu bezpieczeństwa pracy systemu
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wszyscy użytkownicy systemu TI ukończyli szkolenie z zakresu ochrony informacji niejawnych, adekwatne do rodzaju informacji niejawnych przetwarzanych w systemie
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wszyscy użytkownicy zostali wyznaczeni zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wszyscy użytkownicy systemu TI ukończyli szkolenie z zakresu bezpieczeństwa teleinformatycznego, o którym mowa w § 7 RPRM BTI
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wszyscy użytkownicy systemu TI zapoznali się z treścią dokumentu PBE i potwierdzili ten fakt pisemnie
 | **Tak**[ ]  | **Nie**[ ]  |

1. **Zarządzanie bezpieczeństwem informacji:**

|  |  |  |
| --- | --- | --- |
| * 1. Prowadzony jest dziennik pracy administratora systemu, w formie zgodnej z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Prowadzony jest dziennik pracy inspektora bezpieczeństwa teleinformatycznego, w formie zgodnej z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Loginy i hasła administratora systemu (dostępu do BIOS-u, systemu operacyjnego, urządzeń sieciowych) zostały odpowiednio zabezpieczone i zdeponowane zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |

1. **Bezpieczeństwo fizyczne:**

|  |  |  |
| --- | --- | --- |
| * 1. Informacje dotyczące rodzajów, obszaru i lokalizacji stref ochronnych zawarte w zatwierdzonej dokumentacji bezpieczeństwa są zgodne z treścią planu ochrony zatwierdzonego przez kierownika jednostki organizacyjnej
 | **Tak**[ ]  | **Nie**[ ]  |
| **Sygnatura literowo-cyfrowa planu ochrony:**      |
| * 1. Zastosowane środki ochrony fizycznej stref ochronnych są zgodne z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wszystkie strefy ochronne zabezpieczono zgodnie z opisem zawartym w zatwierdzonej dokumentacji bezpieczeństwa systemu TI oraz planie ochrony informacji niejawnych jednostki organizacyjnej
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Dla strefy ochronnej III wprowadzono możliwość kontrolowania osób i pojazdów zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Dla strefy ochronnej II wprowadzono system kontroli wejść i wyjść osób posiadających stałe i czasowe uprawnienia dostępu do tej strefy, zgodny z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Dla strefy ochronnej II wprowadzono system kontroli wejść i wyjść osób nie posiadających stałych lub czasowych uprawnień do przebywania w tej strefie, zgodny z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Dla strefy ochronnej I wprowadzono system kontroli wejść i wyjść osób posiadających stałe i czasowe uprawnienia dostępu do tej strefy, zgodny z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| [ ]  **Nie dotyczy** |
| * 1. Dla strefy ochronnej I wprowadzono system kontroli wejść i wyjść osób nie posiadających stałych lub czasowych uprawnień do przebywania w tej strefie, zgodny z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| [ ]  **Nie dotyczy** |
| * 1. Dla pomieszczenia lub obszaru, w którym zlokalizowane są komponenty systemu TI określono poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zgodnie z § 3 ust. 2 i 3 RRM BF
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Zastosowano środki bezpieczeństwa fizycznego zgodnie z:

[ ]  zapisami RRM BF[ ]  zapisami zarządzenia wydanego w trybie art. 47 ust. 3 UOINadekwatne do wyznaczonego poziomu zagrożeń związanych z utratą poufności, integralności i dostępności informacji niejawnych dla pomieszczenia lub obszaru, w którym będą przetwarzane informacje niejawne w systemie teleinformatycznym  | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Jednostka organizacyjna jest w posiadaniu dokumentów (i/lub certyfikatów) wydanych przez uprawnione osoby lub organizacje, potwierdzających spełnienie przez zastosowane środki bezpieczeństwa fizycznego wymagań zawartych w RRM BF oraz normach określonych w ww. rozporządzeniu lub zarządzeń wydanych w trybie art. 47 ust. 3 UOIN
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Klucze do pomieszczeń, w których znajdują się komponenty systemu TI są przechowywane i prowadzony jest rejestr ich wydawania, zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wejścia do pomieszczeń, w których zlokalizowane są komponenty systemu TI zostały zabezpieczone zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa (drzwi, zamki)
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Okna pomieszczeń, w których zlokalizowane są komponenty systemu TI zostały zabezpieczone, zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wdrożone rozwiązania organizacyjne w zakresie ochrony osobowej (służba ochrony/personel bezpieczeństwa) są zgodne z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Zastosowany system sygnalizacji włamania i napadu (SSWiN) funkcjonuje zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Zastosowany system dozoru wizyjnego (CCTV) funkcjonuje zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Usytuowanie komponentów systemu TI wyklucza możliwość nieuprawnionego podglądu przetwarzanych w systemie informacji niejawnych
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Urządzenia systemu TI zostały właściwie oznaczone i zabezpieczone przed ingerencją do wnętrza urządzeń za pomocą ewidencjonowanych plomb (giloszy)
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Ukompletowanie i lokalizacja komponentów systemu jest zgodna z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Nośniki wykorzystywane do przetwarzania informacji niejawnych zostały oznaczone i zarejestrowane
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Nośniki wykorzystywane do przetwarzania informacji niejawnych są przechowywane zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Wdrożono środki umożliwiające realizację procedur dotyczących sposobu i zasad niszczenia materiałów niejawnych wykorzystywanych w systemie TI, zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. W pomieszczeniach, w których zlokalizowane są komponenty systemu TI nie znajdują się komponenty systemów TI nieujęte w dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Przyjęte rozwiązania organizacyjne zapewniają bezpieczeństwo przetwarzanym informacjom niejawnym w przypadku pracy systemów TI, o których mowna w pkt 15.24, zgodnie z dokumentacją bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |

1. **Bezpieczeństwo teleinformatyczne:**

|  |  |  |
| --- | --- | --- |
| * 1. Dostęp do systemu BIOS/UEFI został zabezpieczony hasłem
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. W systemie BIOS/UEFI wyłączono zbędne urządzenia, porty, interfejsy, zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 |  **Tak** [ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. W systemie BIOS/UEFI ustawiono sekwencję uruchamiania (tj. bootowania) zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Pozostałe ustawienia systemu BIOS/UEFI skonfigurowano zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa (np. w zakresie wyłączenia automatycznego wykrywania urządzeń tj. napędów, nośników)
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Zastosowano ustawienia zabezpieczeń zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 |  |
| * + 1. Zasady haseł
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * + 1. Zasady blokady konta
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * + 1. Zasady inspekcji lub konfiguracja zaawansowanych zasad inspekcji
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * + 1. Przypisywanie praw użytkownika
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * + 1. Opcje zabezpieczeń
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * + 1. Ustawienia logów systemowych
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Uprawnienia do plików systemowych skonfigurowano zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Konta i grupy użytkowników skonfigurowano zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Uprawnienia użytkowników systemu są zgodne z zapisami zatwierdzonej dokumentacji bezpieczeństwa i założeniami zastosowanego w systemie trybu bezpieczeństwa pracy
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Uprawnienia administratora(-ów) systemu są zgodne z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Uprawnienia inspektora(-ów) bezpieczeństwa teleinformatycznego są zgodne z zapisami zatwierdzonej dokumentacji bezpieczeństwa, w tym umożliwiają przeglądanie wszystkich logów systemowych
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Zainstalowane oprogramowanie jest zgodne z wykazem oprogramowania przedstawionym w zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Zainstalowano aktualizacje dostępne dla danej wersji systemu operacyjnego
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Program antywirusowy został skonfigurowany zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Bazy (wzorce) wirusów są aktualne
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Dostęp do portów i usług jest zabezpieczony zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. W urządzeniach sieciowych skonfigurowano np. porty, adresację, tunele, routing zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| [ ]  **Nie dotyczy** |
| * 1. W ustawieniach konfiguracyjnych komponentów systemu (w tym w urządzeniach sieciowych) zapewniono rozliczalność dostępu (tj. osobne konta dla każdego administratora systemu i inspektora bezpieczeństwa teleinformatycznego)
 | **Tak**[ ]  | **Nie**[ ]  |
| [ ]  **Nie dotyczy** |
| * 1. W urządzeniach sieciowych skonfigurowano logi systemowe zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| [ ]  **Nie dotyczy** |

1. **Bezpieczeństwo elektromagnetyczne**:

|  |  |  |
| --- | --- | --- |
| * 1. Dla pomieszczeń, w których zlokalizowane są komponenty systemu TI wyznaczona została Sprzętowa Strefa Ochrony Elektromagnetycznej (SSOE) lub Poziom Zabezpieczenia Miejsca (PZM)

Nr certyfikatu SSOE:      Wyznaczona SSOE: [ ]  SSOE 0 [ ]  SSOE I [ ]  SSOE IINr certyfikatu PZM:      Wyznaczony PZM:[ ]  PZM 0 [ ]  PZM 1 [ ]  PZM 2 [ ]  PZM 3 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Komponenty systemu TI posiadają certyfikaty ochrony elektromagnetycznej. (W przypadku większej ilości urządzeń, poniższe informacje należy przedstawić w załączniku do przedmiotowego wniosku WA-01)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nazwa urządzenia | Zapewniany poziom ochrony | Nr certyfikatu | Data ważności |
| [ ]  | Stacja robocza/jednostka centralna/serwer |  |       |       |
| [ ]  | Monitor |  |       |       |
| [ ]  | Klawiatura |  |       |       |
| [ ]  | Mysz |  |       |       |
| [ ]  | Drukarka/ploter |  |       |       |
| [ ]  | Skaner |  |       |       |
| [ ]  | Szyfrator |  |       |       |
| [ ]  | Dyski twarde |  |       |       |
| [ ]  | UPS |  |       |       |
| [ ]  | Urządzenia sieciowe (np. router, firewall, przełącznik) |  |       |       |
| [ ]  | Inne (np. telefon, fax, mediakonwerter):      |  |       |       |

 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Pozostałe środki ochrony elektromagnetycznej (kabina, obudowa ekranująca itp.) posiadają certyfikaty ochrony elektromagnetycznej

             zapewniany poziom ochrony nr certyfikatu data ważności | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |
| * 1. Wszystkie certyfikaty ochrony elektromagnetycznej są ważne tj. okresowe badania wymagane certyfikatami zostały przeprowadzone i potwierdzone stosownymi dokumentami

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nazwa urządzenia | Model | Nr seryjny | Nr certyfikatu ochrony elektromagne-tycznej | Data ważności (i/lub data ostatniego badania) |
| [ ]  | Kabina |       |       |       |       |
| [ ]  | Obudowa |       |       |       |       |
| [ ]  | Inne |       |       |       |       |

 | **Tak**[ ]  | **Nie**[ ]  |
| **[ ]**  **Nie dotyczy** |

1. **Bezpieczeństwo kryptograficzne:**

|  |  |  |
| --- | --- | --- |
| * 1. W systemie są przekazywane informacje niejawne w formie transmisji poza strefy ochronne
 | **Tak**[ ]  | **Nie**[ ]  |
| **(punkty od 18.2 do 18.8 należy wypełnić w przypadku, gdy w systemie teleinformatycznym są przekazywane informacje niejawne w formie transmisji poza strefy ochronne)** |
| * 1. W systemie teleinformatycznym zastosowano certyfikowane środki ochrony kryptograficznej do transmisji poza strefy ochronne.

Nazwa, typ i model urządzenia lub narzędzia kryptograficznego:      Wersja oprogramowania:      Nr certyfikatu typu:       data ważności:      Nr certyfikatu zgodności:       data ważności:      Nr seryjny urządzenia lub narzędzia kryptograficznego:       | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Ustawienia konfiguracyjne zastosowanych urządzeń lub/i narzędzi kryptograficznych są zgodne z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Ukompletowanie urządzeń lub/i narzędzi kryptograficznych jest zgodne z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Ewidencja materiałów kryptograficznych jest prowadzona zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Materiały kryptograficzne są przechowywane zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Hasła, PIN-kody, karty, moduły uwierzytelniające itp. są zabezpieczone i zdeponowane zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |
| * 1. Urządzenia i/lub narzędzia kryptograficzne są oznakowane i zabezpieczone plombami zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa
 | **Tak**[ ]  | **Nie**[ ]  |

1. **Oświadczenie administratora systemu:**

|  |
| --- |
| Oświadczam, że system teleinformatyczny „     ” został skonfigurowany zgodnie z zapisami zatwierdzonej dokumentacji bezpieczeństwa.  |
| ……………………………………………………(data i czytelny podpis administratora systemu) |

1. **Oświadczenie inspektora bezpieczeństwa teleinformatycznego:**

|  |
| --- |
| Oświadczam, że zweryfikowałem/am konfigurację systemu teleinformatycznego „     ” wykonaną przez administratora systemu. Potwierdzam zgodność konfiguracji systemu z zapisami zatwierdzonej dokumentacji bezpieczeństwa. |
| ……………………………………………………(data i czytelny podpis inspektora bezpieczeństwa teleinformatycznego) |

1. **Oświadczenie kierownika jednostki organizacyjnej:**

|  |
| --- |
| Oświadczam, że wdrożone zostały wszystkie środki ochrony opisane w dokumentacji bezpieczeństwa systemu wskazanej w pkt. 4-6 wniosku oraz mechanizmy bezpieczeństwa określone w pkt. 13.1-18.8 niniejszego wniosku. Oświadczam, że wszystkie informacje zawarte we wniosku są zgodne ze stanem faktycznym. Potwierdzam pełną gotowość jednostki organizacyjnej do wykonania czynności audytowych przez ABW. |

Wnioskodawca zobowiązuje się do pokrycia kosztów przeprowadzenia przez ABW czynności, o których mowa w art. 48 ust. 3-6 UOIN, zgodnie z art. 53 ust. 1 UOIN.

Do wniosku dołączono       str. załączników.

|  |  |
| --- | --- |
| ……………………………………………………(pieczęć firmowa jednostki organizacyjnej) | ……………………………………………………(data i czytelny podpis kierownika jednostki organizacyjnej oraz pieczęć jeśli występuje) |

###### OBJAŚNIENIA I UWAGI

1. Wniosek przesłany do ABW przed zatwierdzeniem dokumentacji bezpieczeństwa systemu teleinformatycznego zostanie odesłany do wnioskodawcy bez rozpatrzenia.
2. Wniosek, w jednym egzemplarzu, należy przesłać do właściwej terytorialnie jednostki organizacyjnej Agencji Bezpieczeństwa Wewnętrznego. Wszelkie odciski pieczęci wnioskodawcy umieszczane na wniosku powinny być wyraźne i czytelne.
3. ABW zastrzega sobie możliwość wystąpienia do wnioskodawcy o dostarczenie dodatkowych dokumentów lub materiałów niezbędnych do przeprowadzenia oceny bezpieczeństwa w ramach prowadzonej akredytacji.
4. Warunkiem rozpoczęcia czynności, o których mowa w art. 48 ust. 6 pkt 2 UOIN jest kompletność dokumentów wymaganych do przeprowadzenia tych czynności. W przypadku stwierdzenia braków formalnych we wniosku lub załączonych dokumentach, wnioskodawca zostanie wezwany do ich uzupełnienia, ze wskazaniem terminu ich uzupełnienia. W przypadku nie usunięcia braków lub nie uzupełnienia wymaganych dokumentów we wskazanym przez ABW terminie, wniosek zostanie odesłany wnioskodawcy bez rozpatrzenia.
5. W przypadku, gdy wnioskodawca, na podstawie art. 53 ust. 3 UOIN będzie ubiegał się o zwolnienie z opłat za czynności, o których mowa w art. 48 ust. 3-6 UOIN, zobowiązany jest dysponować dokumentami uprawniającymi do zwolnienia z ww. opłat.
6. W przypadku, gdy wnioskodawca jest zobowiązany do pokrycia kosztów przeprowadzenia przez ABW akredytacji bezpieczeństwa teleinformatycznego, wnioskodawca otrzyma świadectwo akredytacji po opłaceniu rachunku za przeprowadzone czynności akredytacyjne.
7. Jeśli w pkt. 13.1-18.8, z wyłączeniem punktu 18.1, zaznaczono odpowiedź „NIE” do wniosku należy dołączyć informację uzasadniającą zakreślenie takiej odpowiedzi.
8. W przypadku, gdy kierownik jednostki organizacyjnej powołał więcej niż jednego inspektora bezpieczeństwa teleinformatycznego lub więcej niż jednego administratora systemu należy wymienić wszystkie osoby pełniące te funkcje w formie załącznika do wniosku.
9. W przypadku braku możliwości przeprowadzenia przez ABW (w terminie 90 dni od otrzymania wniosku) audytu bezpieczeństwa systemu teleinformatycznego z winy wnioskodawcy, wniosek WA-01 zostanie odesłany do wnioskodawcy bez rozpatrzenia.
10. Użyte skróty we wniosku:
* UOIN – ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2019.742 z późn. zmianami)
* RPRM BTI – rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948)
* RRM BF – rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U.2012.683)
* ABW – Agencja Bezpieczeństwa Wewnętrznego
* JO – jednostka organizacyjna
* STI, system TI – system teleinformatyczny
* SWB – szczególne wymagania bezpieczeństwa
* PBE – procedury bezpiecznej eksploatacji
* Dokumentacja bezpieczeństwa – dokumentacja, o której mowa w art. 2 pkt 9 UOIN
* AS – administrator systemu
* IBTI – inspektor bezpieczeństwa teleinformatycznego
1. Należy wypełnić w przypadku gdy nadano identyfikator/nazwę/numer stanowiska [↑](#footnote-ref-1)
2. Należy wypełnić w przypadku jednostki organizacyjnej niebędącej jednostką budżetową [↑](#footnote-ref-2)