

PRÓBKA

Bezpłatna próbka z pakietu **Dostawca NIS2 Start** (RealSec). Pełny pakiet zawiera 12 dokumentów w DOCX i PDF oraz przewodnik wdrożenia: politykę, analizę ryzyka, procedurę incydentów i powiadamiania klienta, ciągłość działania, dostęp, podwykonawców, kopie zapasowe, podatności, szkolenia, rejestr aktywów, tę mapę wymagań i checklistę umowną. Odwołania oznaczone strzałką → prowadzą do dokumentów pełnego pakietu. Próbka jest wzorem, nie poradą prawną. Pakiet: sklep.realsec.pl

A-NISD-011

PRÓBKA · v1

[KLASYFIKACJA]

A · ARTEFAKT

PAKIET: DOSTAWCA NIS2 START

Mapa Wymagań Klienta NIS2

30 typowych pytań klienta objętego UKSC: odpowiedź, dokument pakietu, dowód, status

Mapa paruje 30 pytań, które podmioty kluczowe i ważne najczęściej zadają dostawcom ICT w ankietach bezpieczeństwa, negocjacjach umów i audytach, z odpowiedzią wzorcową, dokumentem pakietu i dowodem. Służy do szybkiego i spójnego wypełniania ankiet oraz do wykrywania luk, zanim wykryje je klient.

WŁAŚCICIEL OSOBA ODPOWIEDZIALNA ZA BEZPIECZEŃSTWO CZAS CZYTANIA ≈ 9 MIN	ZATWIERDZA ZARZĄD DOSTAWCY PAKIET DOSTAWCA NIS2 START	OPINIUJE SPRZEDAŻ · KIEROWNICY ZESPOŁÓW	PRZEGLĄD CO 6 MIESIĘCY
--	--	--	----------------------------------

1. Jak korzystać z mapy

Klient objęty ustawą przenosi na Dostawcę wymagania bezpieczeństwa łańcucha dostaw trzema kanałami: ankietą, umową i audytem. Pytania się powtarzają, różni się tylko sformułowanie. Mapa pozwala odpowiadać zawsze tak samo, z dowodem, i od razu widzieć, gdzie Dostawca ma lukę.

1. Dopasuj pytanie z ankiety klienta do najbliższego wiersza mapy (obszar, numer).
2. Użyj odpowiedzi wzorcowej, dostosowując wartości do umowy i faktycznego stanu; nie obiecuj więcej niż wykazuje dowód.

- 3. Dołącz dowód lub zaproponuj jego udostępnienie (np. po podpisaniu umowy o zachowaniu poufności).
- 4. Pytanie bez pasującego wiersza dopisz do mapy na końcu, ze statusem, właścicielem i terminem.
- 5. Ustaw status wiersza: JEST (zdolność działa i jest aktualny dowód), W BUDOWIE (plan z terminem), LUKA (brak zdolności).

STATUS TO DOWÓD

Wszystkie wiersze mają domyślnie status [DO USTALENIA]. Przed pierwszym użyciem Dostawca ustawia statusy według faktycznego stanu. Status JEST bez aktualnego dowodu nie istnieje, a odpowiedź wzorcowa opisuje stan docelowy po wdrożeniu pakietu, nie stan bieżący.

2. Mapa 30 pytań

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
1	Status	Czy są Państwo podmiotem kluczowym lub ważnym w rozumieniu UKSC?	Nie: ocena wg art. 2 pkt 4i-4j i art. 5 UKSC (MSSP kluczowy od małego przedsiębiorcy; MSP, chmura, centrum danych od średniej wielkości) wykazała, że nie spełniamy kryteriów; przegląd co 12 mies. Jeśli ocena wykaże inaczej, ten pakiet nie wystarcza.	→ L1-NISD-001 · Polityka Bezpieczeństwa Informacji Dostawcy	Notatka z oceny statusu z datą i uzasadnieniem	[DO USTALENIA]

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
2	Status	Kto u Państwa odpowiada za cyberbezpieczeństwo i jak się z nim skontaktować?	Osoba odpowiedzialna i zastępca wskazani z imienia i nazwiska; kontakt incydentowy i awaryjny	→ L1-NISD-001 • Polityka Bezpieczeństwa Informacji Dostawcy	Polityka z rolami, lista kontaktów	[DC USTALE
3	Polityka	Czy mają Państwo zatwierdzoną politykę bezpieczeństwa informacji?	Tak, zatwierdzona przez Zarząd, przegląd co 12 mies.	→ L1-NISD-001 • Polityka Bezpieczeństwa Informacji Dostawcy	Polityka z datą zatwierdzenia	[DC USTALE
4	Polityka	Jak realizują Państwo środki z art. 8 ust. 1 pkt 2 UKSC (art. 21 ust. 2 NIS2)?	Mapa 14 obszarów (lit. a-n) na dokumenty i dowody	→ L1-NISD-001 • Polityka Bezpieczeństwa Informacji Dostawcy	Tabela obszarów (rozdz. 5 polityki)	[DC USTALE
5	Polityka	Czy posiadają Państwo certyfikat ISO/IEC 27001?	Jeśli tak: certyfikat z zakresem. Jeśli nie: stosujemy środki odpowiadające wybranym zabezpieczeniom ISO/IEC 27001, bez deklaracji zgodności z normą, z dowodami działania	→ L1-NISD-001 • Polityka Bezpieczeństwa Informacji Dostawcy	Certyfikat i zakres albo zestaw dowodów z tej mapy	[DC USTALE
6	Ryzyko	Czy przeprowadzają Państwo analizę ryzyka usług świadczonych nam?	Tak, co 12 mies. i po istotnych zmianach, w perspektywie Dostawcy i klienta	→ L2-NISD-002 • Analiza Ryzyka i Rejestr Ryzyk	Rejestr ryzyk, data analizy, wyciąg dla usługi klienta	[DC USTALE

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
7	Ryzyko	Jak postępują Państwo z ryzykami wysokimi?	Eskalacja do Zarządu w 2 dni rob., plan w 10 dni rob.; akceptacja wyjątkowo, maks. 6 mies.	→ L2-NISD-002 • Analiza Ryzyka i Rejestr Ryzyk	Decyzje Zarządu, status planów	[DC USTALE
8	Incydenty	W jakim czasie poinformują nas Państwo o incydencie dotyczącym naszej usługi?	Incydent poważny: ≤ 2h od wykrycia w oknie serwisowym, poza nim do ustalonej godziny następnego dnia roboczego, 24/7 przy dyżurze zapisanym w umowie; aktualizacje co 4h; raport przyczyn ≤ 10 dni rob.	→ L3-NISD-003 • Procedura Obsługi Incydentów i Powiadamiania Klienta	Procedura, wyciąg z rejestru incydentów z czasami powiadomień	[DC USTALE
9	Incydenty	Czy dostarczą Państwo informacje potrzebne do naszego zgłoszenia w S46 (24h, 72h, 1 mies.)?	Tak: komunikat wstępny z polami z art. 12 ust. 1 UKSC, dane do zgłoszenia i sprawozdania końcowego na żądanie; ćwiczenie stolikowe co 12 mies.	→ L3-NISD-003 • Procedura Obsługi Incydentów i Powiadamiania Klienta	Wzór komunikatu, przykładowy raport przyczyn, protokół ćwiczenia	[DC USTALE

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
10	Kryptografia	Czy szyfrują Państwo nasze dane w spoczynku i w transmisji?	Tak: TLS 1.3 lub 1.2 w transmisji, szyfrowanie dysków i baz z danymi klientów; nowe klucze RSA ≥ 3072 bitów, ECDSA lub Ed25519 dla podpisów; sekrety w menedżerze sekretów	→ L1-NISD-001 • Połityka Bezpieczeństwa Informacji Dostawcy	Konfiguracja, wynik skanu TLS, raport szyfrowania urządzeń	[DC USTALE
11	Monitorowanie	Czy monitorują Państwo systemy świadczące nam usługę i jak długo przechowują logi?	Logi i alerty bezpieczeństwa systemów usług objętych; przegląd w oknie serwisowym, 24/7 przy dyżurze; retencja logów co najmniej 12 mies.	→ L1-NISD-001 • Połityka Bezpieczeństwa Informacji Dostawcy	Konfiguracja alertów i retencji, przykładowy raport	[DC USTALE
12	Ciągłość	Jakie są RTO i RPO naszej usługi i kiedy były testowane?	Klasa A: $RTO \leq 24h$, $RPO \leq 4h$; klasa B: $RTO \leq 5$ dni rob., $RPO \leq 24h$, lub wartości z umowy; test klasy A co 12 mies.	→ L2-NISD-004 • Standard Ciągłości Działania i Odtwarzania Usług	Przypisanie usługi do klasy, streszczenie raportu z testu	[DC USTALE
13	Dane	Gdzie przetwarzają Państwo nasze dane i jak spełniają wymagania RODO?	Lokalizacje z rejestru (kraje, regiony chmury), umowa powierzenia, lista podprocesorów, zgłaszanie naruszeń bez zbędnej zwłoki (art. 33 ust. 2 RODO)	→ A-NISD-010 • Rejestr Aktywów i Usług	Wyciąg z rejestru, umowa powierzenia, lista podprocesorów	[DC USTALE

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
14	Kopie	Jak chronią Państwo kopie zapasowe przed ransomware i jak często je wykonują?	Reguła 3-2-1+1, kopia niemodyfikowalna lub offline, odrębne konta z MFA; klasa A: przyrostowo co 4h, pełna dobowo, 35 dni; klasa B: dobowo, 30 dni	→ L2-NISD-007 • Standard Kopii Zapasowych i Odtwarzania	Opis schematu kopii, raport skuteczności zadań	[DC USTALE
15	Fizyczne	Jak zabezpieczają Państwo fizycznie serwery, biuro i nośniki z naszymi danymi?	Zamknięte pomieszczenia z ewidencją dostępu, centra danych podwykonawców z potwierdzonymi zabezpieczeniami, czyste biurko, bezpieczne niszczenie nośników	→ L1-NISD-001 • Polityka Bezpieczeństwa Informacji Dostawcy	Opis zabezpieczeń, certyfikat centrum danych, protokoły niszczenia	[DC USTALE
16	Dostęp	Czy stosują Państwo uwierzytelnianie wieloskładnikowe?	MFA dla 100% dostępów zdalnych, poczty, repozytoriów, konsol chmurowych, systemów klientów i kont uprzywilejowanych	→ L2-NISD-005 • Standard Zarządzania Dostępem	Raport pokrycia MFA	[DC USTALE
17	Dostęp	Kto z Państwa strony ma dostęp do naszych systemów i jak jest on kontrolowany?	Rejestr osób uprawnionych, kanał uzgodniony z klientem, rejestrowanie sesji, przegląd co 3 mies.	→ L2-NISD-005 • Standard Zarządzania Dostępem	Rejestr osób uprawnionych, protokół przeglądu	[DC USTALE

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
18	Dostęp	Jak szybko odbierają Państwo dostęp osobom odchodzącym?	≤ 24h od ustania współpracy, z informacją do klienta	→ L2-NISD-005 • Standard Zarządzania Dostępem	Próbka procesu odejścia	[DC USTALE
19	Podatności	W jakim czasie usuwają Państwo podatności krytyczne?	Systemy z internetu ≤ 72h, pozostałe ≤ 7 dni; aktywnie wykorzystywane bez poprawki: środki kompensujące ≤ 24h	→ L3-NISD-008 • Procedura Aktualizacji i Zarządzania Podatnościami	Zestawienie podatności, rejestr wyjątków	[DC USTALE
20	Podatności	Jak informują nas Państwo o podatnościach w dostarczonym oprogramowaniu?	Informacja z oceną wpływu i terminem poprawki; aktywnie wykorzystywane w trybie incydentu	→ L3-NISD-008 • Procedura Aktualizacji i Zarządzania Podatnościami	Przykładowe powiadomienie, notatki wydań	[DC USTALE
21	Wytwarzanie	Jakie praktyki bezpiecznego wytwarzania i testów Państwo stosują?	Przegląd kodu, SAST, SCA, ochrona sekretów, zabezpieczony potok CI/CD, SBOM; pentest usług klasy A co 12 mies.	→ L3-NISD-008 • Procedura Aktualizacji i Zarządzania Podatnościami	Opis praktyk, raport SCA, SBOM, streszczenie pentestu	[DC USTALE
22	Personel	Czy pracownicy mają zobowiązania do poufności i jak są weryfikowani?	Zobowiązanie do poufności w umowie; osoby realizujące u klienta zadania z art. 8 lub 11 UKSC przedstawiają informację z KRK (art. 8f); inna weryfikacja tylko w granicach prawa pracy i RODO	→ L2-NISD-009 • Standard Szkoleń i Świadomości Bezpieczeństwa	Wzór zobowiązania, lista osób z datą informacji z KRK	[DC USTALE

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
23	Łańcuch dostaw	Z jakich podwykonawców Państwo korzystają przy naszej usłudze?	Lista podwykonawców usługi z klasą, lokalizacją danych i oceną	→ L2-NISD-006 • Standard Bezpieczeństwa Łańcucha Dostaw	Wyciąg z rejestru podwykonawców	[DC USTALE
24	Łańcuch dostaw	Jak oceniają i nadzorują Państwo swoich podwykonawców?	Ocena przed umową i co 12 mies., przegląd po incydencie, sprawdzenie decyzji o dostawcy wysokiego ryzyka (art. 67b), klauzule przeniesione z umowy klienta	→ L2-NISD-006 • Standard Bezpieczeństwa Łańcucha Dostaw	Daty i wyniki ocen, wzór klauzul	[DC USTALE
25	Łańcuch dostaw	Czy poinformują nas Państwo o zmianie podwykonawcy?	Podwykonawca istotny: ≥ 30 dni (klasa A), ≥ 14 dni (pozostałe), zmiana lokalizacji danych ≥ 30 dni; dłużej do uzgodnienia; zmiana wymuszona niezwłocznie	→ L2-NISD-006 • Standard Bezpieczeństwa Łańcucha Dostaw	Historia powiadomień	[DC USTALE
26	Aktywa	Czy prowadzą Państwo inwentaryzację systemów używanych do świadczenia usługi?	Rejestr usług i aktywów z właścicielami, klasami i datą przeglądu	→ A-NISD-010 • Rejestr Aktywów i Usług	Wyciąg z rejestru	[DC USTALE
27	Szkolenia	Czy pracownicy przechodzą szkolenia z bezpieczeństwa?	Wstępne ≤ 14 dni, roczne dla wszystkich (cel ≥ 98%), rolowe, phishing co 6 mies.	→ L2-NISD-009 • Standard Szkoleń i Świadomości Bezpieczeństwa	Wyciąg z rejestru szkoleń, wyniki phishingu	[DC USTALE

NR	OBSZAR	PYTANIE KLIENTA	ODPOWIEDŹ WZORCOWA (SKRÓT)	DOKUMENT	DOWÓD	STATUS
28	Szkolenia	Czy kierownictwo odbywa szkolenia z cyberbezpieczeństwa?	Tak, co 12 mies., dobrowolnie na wzór art. 8e UKSC	→ L2-NISD-009 · Standard Szkoleń i Świadomości Bezpieczeństwa	Potwierdzenie szkolenia Zarządu	[DC USTALE
29	Umowa	Czy akceptują Państwo nasze klauzule bezpieczeństwa łańcucha dostaw?	Stanowisko według checklisty: akceptuj, negocjuj, granica	→ T-NISD-012 · Checklista Umowna NIS2 dla Dostawcy	Wypełniona checklista umowna	[DC USTALE
30	Umowa	Czy umożliwią Państwo audyt lub przekażą dowody zgodności?	Tak: najpierw pakiet dowodów, następnie audyt zdalny, audyt na miejscu w uzgodnionym trybie; odpowiedź na żądanie dowodu w 5 dni rob.	→ T-NISD-012 · Checklista Umowna NIS2 dla Dostawcy	Pakiet dowodów z tej mapy, klauzula audytu	[DC USTALE

3. Pokrycie obszarów art. 8 UKSC

UKSC ART. 8 UST. 1	NIS2 ART. 21 UST. 2	PYTANIA W MAPIE
pkt 1, pkt 2 lit. a: ryzyko i polityki	lit. a	3, 4, 5, 6, 7
pkt 2 lit. b, pkt 5: nabywanie, rozwój, aktualizacje, podatności	lit. e	19, 20, 21
pkt 2 lit. c: bezpieczeństwo fizyczne	ust. 2 wstęp	15
pkt 2 lit. d: zasoby ludzkie	lit. i	18, 22
pkt 2 lit. e i ust. 2: łańcuch dostaw	lit. d, ust. 3	23, 24, 25, 29
pkt 2 lit. f: ciągłość i kopie	lit. c	12, 14

UKSC ART. 8 UST. 1	NIS2 ART. 21 UST. 2	PYTANIA W MAPIE
pkt 2 lit. g: monitorowanie ciągłe	brak odrębnej litery	11
pkt 2 lit. h: ocena skuteczności	lit. f	12 (test odtworzenia), 30 (dowody i audyt)
pkt 2 lit. i i j: edukacja, cyberhigiena	lit. g	27, 28
pkt 2 lit. k: kryptografia	lit. h	10
pkt 2 lit. l: bezpieczna komunikacja, MFA	lit. j	16
pkt 2 lit. m: aktywa	lit. i	26, 13
pkt 2 lit. n: kontrola dostępu	lit. i	16, 17, 18
pkt 4: incydenty	lit. b	8, 9
Status Dostawcy, kontakt, RODO, umowa	nie dotyczy	1, 2, 13, 29, 30

4. Pułapki przy odpowiadaniu

PUŁAPKA	JAK ODPOWIEDZIEĆ
Klient żąda powiadomienia "w 1h od wystąpienia" incydentu, całą dobę	Termin może być tylko od wykrycia; zaproponuj ≤ 2h od wykrycia w oknie serwisowym, a całodobowo tylko jako płatny dyżur 24/7. Nie obiecuj terminu, którego nie umiesz zmierzyć.
Pytanie o certyfikat ISO/IEC 27001, którego Dostawca nie ma	Nie deklaruj zgodności z normą; pokaż dowody działania środków z tej mapy i, jeśli to prawda, plan certyfikacji.
Klient pyta o status Dostawcy w UKSC, a ocena nie była zrobiona	Zrób ocenę według polityki (rozdz. 3) przed odpowiedzią; błędna deklaracja statusu jest gorsza niż jej brak.
Żądanie nieograniczonego audytu na miejscu w środowisku współdzielonym z innymi klientami	Akceptuj prawo audytu co do zasady, negocjuj tryb: najpierw dowody, potem audyt zdalny, na miejscu z ochroną danych innych klientów.
Różne odpowiedzi na to samo pytanie dla różnych klientów	Zawsze z mapy; odstępstwo tylko z przyczyny umownej i z adnotacją w mapie.

5. Utrzymanie mapy

- Przegląd mapy co 6 mies. i po każdej nowej ankiecie zawierającej pytanie spoza mapy.
- Przy przeglądzie sprawdź datę każdego dowodu: dowód starszy niż 12 mies. zmienia status na W BUDOWIE do czasu odświeżenia.
- Luki (LUKA, W BUDOWIE) z właścicielem i terminem raportuje się Zarządowi w przeglądzie zarządczym (→ L1-NISD-001 · Polityka Bezpieczeństwa Informacji Dostawcy).
- Odpowiedź na żądanie dowodu od klienta: w 5 dni rob.; ankieta krótka ≤ 5 dni rob., pełna ≤ 10 dni rob.

6. Status dokumentu

Dokument jest elementem pakietu **Dostawca NIS2 Start** (RealSec, wersja pakietu v1) i ma status PROJEKT do czasu zatwierdzenia przez Zarząd Dostawcy. Klasyfikację dokumentu nadaje Dostawca: [KLASYFIKACJA].

Dokument jest wzorem (szablonem). Przed przyjęciem wymaga dostosowania do faktycznej organizacji, usług, umów i ryzyk Dostawcy, przeglądu prawnego oraz zatwierdzenia przez kierownictwo. Nie stanowi porady prawnej ani gwarancji zgodności z przepisami lub oczekiwaniami klienta czy organu. Stan prawny: 2026-10-07.

WERSJA	DATA	AUTOR	OPIS ZMIANY
1	2026-10-07	RealSec	Pierwsze wydanie w pakiecie Dostawca NIS2 Start (projekt).

7. Załącznik: źródła w bibliotece RealSec

Dokument opracowano jako wersję uproszczoną i samodzielną na bazie dokumentów biblioteki RealSec: A-VND-109, T-VND-110, T-VND-111, A-KSC-009. Kody służą wyłącznie identyfikowalności; do stosowania pakietu nie są potrzebne.