Kwestionariusz dla dostawców NIS 2

Otwarty, zakotwiczony w prawie UE kwestionariusz do oceny dostawców w ramach NIS 2

Wersja 3.1.0 - Ostatnia aktualizacja 2026-05-15 - 59 pól w 6 sekcjach

Ka ÆFP pole jest zakotwiczone w pierwotnym §/6FÆP na poziomie UE: NIS 2 Art. 21(2), CIR 2024/2690, ENISA Technical Implementation Guidance, GDPR Art. 28 lub Cyber Resilience Act. Uzupe &æ–Væ– sektorowe (TISAX, VDA ISA, BSI C5, KRITIS) s R FöF wane do tej podstawy.

—/6ABo: github.com/NISD2/nis2-supply-chain-questionnaire-schema (MIT + CC BY 4.0)

1. Profil dostawcy (18 pól)

Nazwa prawna

[string] Wymagane - Podstawa prawna: ENISA TIG §5.2
Zarejestrowana nazwa Twojej firmy, taka jak widnieje w rejestrze handlowym. Przyk & C Müller GmbH lub Acme Software Ltd.

Adres siedziby

[string] Wymagane - Podstawa prawna: ENISA TIG §5.2
Zarejestrowany adres prowadzenia dzia & Æaeñ[ci Twojej firmy. Wystarczy jeden adres, nawet je ¶Æ' Ö 7¢ ¶–Æ¶ Æö¶ Æ—¦ 6¦'à

Kraj

[country] Wymagane - Podstawa prawna: ENISA TIG §5.2
Kraj, w którym Twoja firma ma siedzib ' awn Rà Dwie litery, np. DE dla Niemiec.

Domena g /0wna

[url] Opcjonalne - Podstawa prawna: ENISA TIG §5.2(b)
Twoja domena g /0wna, zwykle adres URL Twojej witryny. Przyk & C acmesoftware.com.

Slogan (jedna linia, widoczny dla klientów)

[string] Opcjonalne - Podstawa prawna: ENISA TIG §5.2(b)
Jedna linia podsumowuj V6 Twoj R ö`ert 'à Klienci widz R ¡ w Twoim profilu dostawcy. Przyk & C ERP dla produkcji w sektorze M ¥.

Opis publiczny (d 'Q|szy)

[text] Opcjonalne - Podstawa prawna: ENISA TIG §5.2(b)
Dwa do trzech zda @ o Twojej firmie i tym, czym si • zajmuje. Pojawia si • to w Twoim profilu dostawcy. Argumentacja sprzeda Æðwa, postawa w zakresie bezpiecze G7Gpa lub oba elementy.

Opis ·v– F7¦öàych us 'Vp

[text] Wymagane - Podstawa prawna: ENISA TIG §5.2(b) + §5.1.4 TIPS
Jeden akapit o tym, co Twoja firma technicznie dostarcza klientom. Konkretne produkty, modu '• lub us 'Vv'à Unikaj czysto marketingowego j —§–¶ à

Kraje / regiony, w których przetwarzane s R F æR ¶Æ–VçO0w

[string] Wymagane - Podstawa prawna: ENISA TIG §5.1.4 TIPS
Wszystkie kraje, w których przechowywane lub przetwarzane s P dane Twoich klientów. Oddzielone przecinkami, kody krajów ISO. Przyk & C DE, NL, US. Je ¶Æ' ' etwarzasz dane wy ! cznie w UE, wystarczy wymieni r · aje UE.

Imi ' ' æ §v—6°o kontaktu ds. bezpiecze G7Gv

[string] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(d)
Osoba, z któr P klienci kontaktuj P si • w przypadku incydentu bezpiecze G7Gpa. W mniejszych firmach cz —7Fð dyrektor zarz VG¦ ¡ lub kierownik IT. Wystarczy jedna osoba.

E-mail kontaktowy do zg & 7¦ æ– –æ0ydentów

[email] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(d)
Adres e-mail, którego klienci u Ç—paj P do zg & 7¦ æ– incydentu bezpiecze G7Gpa. Najlepiej lista dystrybucyjna, taka jak security@example.com, która dociera do wielu osób.

Telefon kontaktowy do zg & 7¦ æ– –æ0ydentów (24/7)

[phone] Opcjonalne - Podstawa prawna: CIR 2024/2690 §5.1.4(d)
Numer telefonu do pilnych zg &÷7 e B –æ7–FVçO0w. Je ¶Æ' æ–R &ðwadzisz dy ÇW u 24/7, podaj godziny pracy w nawiasie.

SLA powiadamiania o incydentach (godziny)

[integer] Opcjonalne - Podstawa prawna: NIS2 Art. 23
Liczba godzin od wykrycia incydentu do powiadomienia klienta, najpó ¦æ–V¢à Realistyczna samoocena, a nie warto ± docelowa. Typowe warto ¶6" 24, 48 lub 72 godziny.

Identyfikator rejestracji BSI (tylko je ¶Æ' Twoja firma sama podlega NIS2)

[string] Opcjonalne - Podstawa prawna: ENISA TIG §5.1.2
Je ¶Æ• Twoja firma sama podlega NIS 2 i jest zarejestrowana w BSI, wpisz tutaj identyfikator rejestracji. Opcjonalne. Pozwala klientom od razu zobaczy rÂ |e spe &æ– 7¢ FVâ 6 Ò ö&ðwi W ek co podmiot regulowany.

§v– F7§–Ðy us 'Vv' 6 2 ò †÷7Fðwane

[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.2(b)
Uruchamiasz oprogramowanie dla klientów na w & 6æV infrastrukturze i dostarczasz je przez internet. Zaznacz wi –6V ni À jedno pole, je ¶Æ' ö`erujesz kilka modeli.

Dostarczamy oprogramowanie on-premise
[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.2(b)
Dostarczasz oprogramowanie, które klienci instaluj R ’ W uchamiaj R æ qBasnej infrastrukturze.

§v– F7§–Ðy us 'Vv’ ofesjonalne / doradztwo
[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.2(b)
Twoim g /0wnym produktem jest praca ludzka: doradztwo, wdro ÆVæ–P, szkolenia, audyt lub dostosowanie.

§v– F7§–Ðy us 'Vv’ ¦ '¡ dzane / MSP
[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.2(b)
Obs 'VwV¦W7¢ FÆ ¶Æ–VçF 7¡ ¶6’ ¦Vvò –æg astruktury IT, w & 6àym personelem. Typowe dla modeli MSP i MSSP.

U Ç—v Ðy, integrujemy lub dostarczamy systemy SI
[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(d)
Czy Twoje produkty lub us 'Vv• przetwarzaj P dane klientów za pomoc P modelu SI lub ML? Obejmuje to modele zewn —G'¦æP wywo '—pane przez API, na przyk & B ÷ Vä ’ ÇV" çF‡&÷ –2à

2. Praktyki bezpiecze G7Gv ƒ#b 6Â•

Udokumentowany system zarz VG¦ æ– &W§ –V7 e G7GvVÒ –æ`ormacji (ISMS)
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.2(a)
Zaznacz tak, je ¶Æ• masz pisemn P polityk • bezpiecze G7Gpa informacji z przypisanymi rolami, regularnymi przegl VF Ö• i udokumentowan R ö'1Bug R –æ7–FVçO0w. Certyfikacja ISO 27001 lub BSI Grundschutz oznacza tak.

Posiadanie certyfikatu ISO 27001, BSI Grundschutz lub równowa ÆæVvð
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.2(b)
Zaznacz tak, je ¶Æ• Twoja firma posiada aktualnie certyfikat ISO 27001, BSI Grundschutz, SOC 2 Type II lub równowa Æày. Prze ¶Æ–¢ 6W tyfikat w zak & F6R 6W tyfikaty.

Coroczne szkolenie z zakresu ·v– FöÖñ[ci bezpiecze G7Gv FÆ 6 Bego personelu
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(b)
Zaznacz tak, je ¶Æ• ka ÆG• pracownik otrzymuje co najmniej jedno coroczne szkolenie z zakresu ·v– FöÖñ[ci bezpiecze G7Gpa informacji. E-learning si ’ Æ–7§“° symulacje phishingu s R W§W QBnieniem.

Weryfikacja przesz &ñ[ci personelu z dost — VÒ Fò F àych klientów
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(c)
Zaznacz tak, je ¶Æ• przeprowadzasz weryfikacj • przesz &ñ[ci personelu z dost — VÐ do danych klientów. Typowy poziom: wyci Vp z rejestru karnego lub równowa Æày dokument przy zatrudnieniu.

Udokumentowany proces obs 'Vv’ öF Fæñ[ci i instalowania poprawek
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(f)
Zaznacz tak, je ¶Æ• masz pisemny proces obs 'Vv• podatno ¶6• bezpiecze G7Gpa: wykrywanie, ocena, priorytetyzacja, instalowanie poprawek lub & vöG enie. Monitorowanie CVE i instalowanie poprawek w oparciu o SLA s R 7F æF &FVÒà

Akceptacja prawa klienta do audytu (lub udost — æ– æ–R & ÷ tów z audytu)
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(e)
Zaznacz tak, je ¶Æ• przyznajesz klientom prawo do audytu na miejscu albo udost — æ– 7 zast — 7 e raporty z audytu (na przyk & @ SOC 2, ISAE 3402).

Korzystanie z podwykonawców przetwarzania / poddostawców
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(g)
Zaznacz tak, je ¶Æ• do ·v– F7 enia us 'Vv• korzystasz z innych firm, które maj P dost — do danych lub infrastruktury klientów. Typowe przyk & G“ AWS, Azure, Cloudflare, Stripe.

Lista podwykonawców przetwarzania
[text] Warunkowe - Podstawa prawna: CIR 2024/2690 §5.1.4(g)
Wymie @ ka ÆFVvð podwykonawc • przetwarzania z nazw RÀ miejscem przetwarzania i tym, co dla Ciebie robi. Wystarczy tabela lub lista punktowana. Aktualizuj j R ¦ ¶ |dym razem, gdy dodajesz lub usuwasz podwykonawc ’à

Zobowi W¦ æ–R Fò §w otu / zniszczenia danych klientów po zako F7 eniu umowy
[boolean] Wymagane - Podstawa prawna: CIR 2024/2690 §5.1.4(h)
Zaznacz tak, je ¶Æ• zobowi W§V¦W7 si • umownie do zwrotu lub zniszczenia danych klientów po zako F7 eniu umowy. Powszechna praktyka: eksport i zwrot, a nast — æ–R W7Væ‘ cie w ci VwR 3 Fæ’à

Dost — æ 7F æF dowa umowa o przetwarzaniu danych (DPA)
[boolean] Wymagane - Podstawa prawna: GDPR Art. 28
Zaznacz tak, je ¶Æ• masz standardow P umow • o przetwarzaniu danych zgodnie z artyku &VÐ 28 GDPR, któr P klienci mog P podpisa Wymagane, gdy tylko przetwarzasz dane osobowe.

Polityki bezpiecze G7Gv 1 przegl VF æR 6ò æ ¦Öæ–V¢ & ¢ r oku
[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(a) / ENISA TIG §1.1
Zaznacz tak, je ¶Æ• Twoje polityki bezpiecze G7Gpa s P przegl VF æP co najmniej raz w roku i aktualizowane w razie potrzeby. Pisemna notatka w dokumencie jest wystarczaj V7–Ò Fðwodem.

Udokumentowany plan reagowania na incydenty

[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(b) / ENISA TIG §3

Zaznacz tak, je ¶Æ• masz pisemny plan obs 'Vv• incydentów bezpiecze G7Gpa: kto decyduje, kto komunikuje, kto dokumentuje. Co najmniej jedno wv–7 enie sztabowe rocznie to dobra praktyka.

Udokumentowany plan ci VqBo ¶6’ G¦– Bania / odtwarzania po awarii

[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(c) / ENISA TIG §4

Zaznacz tak, je ¶Æ• masz plan wyja ¶æ– ¡ cy, jak utrzymujesz dzia & æ–P lub szybko przywracasz je podczas awarii: systemy krytyczne, rozwi W¦ æ– waryjne, cele RTO i RPO.

Udokumentowana polityka kryptografii

[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(h) / ENISA TIG §9

Zaznacz tak, je ¶Æ• masz pisemnie okre ¶ÆöæP, jak P kryptografi • stosujesz i gdzie: dane w tranzycie (TLS 1.2+), dane w spoczynku (AES-256), zarz VG¦ æ–R ¶ÇV7¦ Ö’Â Æv÷ ytmy haszuj V6P.

Zarz VG¦ æ–R F÷7A pem uprzywilejowanym (PAM) dla personelu wewn —G'¦æVvð

[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Zaznacz tak, je ¶Æ• administratorzy i konta uprzywilejowane maj P dodatkowe mechanizmy kontroli: osobne logowanie, MFA, rejestrowanie sesji lub dost — §W7BÖ–â×F–ÖP.

MFA wymuszone dla wszystkich wewn —G'¦àych kont administracyjnych / uprzywilejowanych

[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(j)

Zaznacz tak, je ¶Æ• ka ÆFP wewn —G'¦æP konto administracyjne lub uprzywilejowane musi u Ç—pa p MFA. Tokeny sprz —Fðwe lub a uwierzytelniaj V6R 6‘ licz S° SMS nie.

Prowadzenie inwentaryzacji zasobów informacyjnych

[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(i) / ENISA TIG §12.4

Zaznacz tak, je ¶Æ• prowadzisz aktualn P list • ka ÆFVvð systemu informacyjnego u Ç—panego do ·v– F7 enia us 'Vv“ serwery, ba danych, narz –G¦– 6 0, punkty ko F6ðwe. Wystarczy arkusz kalkulacyjny.

Program testów penetracyjnych co rok lub co dwa lata

[boolean] Wymagane - Podstawa prawna: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Zaznacz tak, je ¶Æ• zlecasz zewn —G'¦ày test penetracyjny co najmniej raz na jeden do dwóch lat. W przypadku mniejszych firm akceptowalnym minimalnym krokiem jest zewn —G'¦æR 6¶ æðwanie podatno ¶6’à

Ujawniamy przesz &R öFÆVv ¡ ce zg &÷7 eniu zdarzenia cyberbezpiecze G7Gv æ o ¶! klientów

[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.1.2

Zaznacz tak, je ¶Æ• na pro ¶! klienta otwarcie ujawniasz, czy i jakie podlegaj V6P zg &÷7 eniu incydenty bezpiecze G7Gpa Twoja firma mia & r ' esz &ñ[ci. Typowy okres: ostatnie od trzech do pi –6—R Æ Bà

Zapewniamy klientom pomoc w razie incydentu bez kosztów / po kosztach ustalonych z góry

[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.1.4 TIPS

Zaznacz tak, je ¶Æ• zobowi W§V¦W7 si • pomaga p klientom bez dodatkowych kosztów, gdy incydent jest spowodowany przez Twój produkt lub us 'Vq . Je ¶Æ’ ¦ Ö– 7B FVvò ¢ •7 y uzgadniasz wcze ¶æ–V¢ ¦FVf–æ–ðwan R 7F wk ’ G¦–Væá , równie Â ¦ ¦æ 7¢ F ²à

Pe &æ w7 1Bpraca z w & [ciwymi organami (BSI, ENISA, krajowe CSIRT)

[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.1.4 TIPS

Zaznacz tak, je ¶Æ• zobowi W§V¦W7 si • do pe &æV wspó ' acy z w & [ciwymi organami, takimi jak BSI, ENISA lub krajowe CSIR podczas inspekcji, audytów i obs 'Vv’ –æ7–FVçO0w. Standard dla powa Æàych dostawców.

Powiadamiamy klientów o ka ÆFV¢ —7F÷FæV¢ ¦Ö– æ–R w Bywaj V6V¢ æ [wiadczenie us 'Vv•

[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.1.4 TIPS

Zaznacz tak, je ¶Æ• zobowi W§V¦W7 si • powiadamia p klientów o ka ÆFV istotnej zmianie wp '—paj V6V na Twoj P zdolno ± do us 'Vv“ przej –6– Â ¦Ö– ày podwykonawcy przetwarzania, powa ÆæR ¦Ö– ày techniczne.

Powiadamiamy klientów z wyprzedzeniem, je ¶Æ’ ¦Ö–Væ– ¡ si ’ Ö–V§66 ' etwarzania danych

[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.1.4 TIPS

Zaznacz tak, je ¶Æ• informujesz klientów z wyprzedzeniem, zanim zmieni si • miejsce przetwarzania ich danych. Wa ÆæP dla ochrony danych i dla zgodnego z GDPR nadzoru nad & Dcuchem dostaw.

Udokumentowana strategia wyj ¶6– ¢ ö&ðwi W¦°owym okresem przej ¶6–ðwym

[boolean] Wymagane - Podstawa prawna: ENISA TIG §5.1.4 TIPS

Zaznacz tak, je ¶Æ• masz pisemn P strategi • wyj ¶6– jak d 'Vvð trwa uporz VF°owane przekazanie, jakie dane i wiedza s przekazywane, do czego si ’ obowi W§V¦W7¢ r ö·&W6–R ' ej ¶6–ðwym.

Dostarczamy SBOM-for-AI zgodnie z minimalnymi elementami G7

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

Opcjonalne. Zaznacz tak, je ¶Æ• mo ÆW7 dostarczy p SBOM-for-AI zgodnie z minimalnymi elementami G7 (maj 2026). Dokumentuje metadane, modele, dane treningowe, infrastruktur ’À w & [ciwo ¶6• bezpiecze G7Gpa, KPI i zachowanie systemu. Standard dobrowolny.

URL dokumentu SBOM-for-AI

[url] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(d) / ENISA TIG §5.1.2

Publiczny lub udost — æ–öày URL do Twojego dokumentu SBOM-for-AI. Mo ÆR Fò y r Æ–² D`, plik JSON lub strona projektu.

3. Specyficzne dla SaaS (5 pól)

Region hostingu

[string] Warunkowe - Podstawa prawna: ENISA TIG §5.2

Region chmury, w którym hostowane s P dane klientów. Przyk & C AWS eu-central-1, Azure West Europe. Podaj region g /0wny; regiony zapasowe lub do tworzenia kopii zapasowych mo Ææ FöF po przecinku.

Szyfrowanie danych w spoczynku

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(h) / ENISA TIG §9

Zaznacz tak, je ¶Æ• dane klientów na dysku s P szyfrowane w spoczynku za pomoc P AES-256 lub równowa ÆæVvð standardu. Liczy si ' 7§–g&ðwanie dysków zarz VG¦ æR ' ez chmur ' „ WS EBS, Azure Disk Encryption).

Szyfrowanie podczas przesy & æ– …DÅ2 &R ã"•

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(h) / ENISA TIG §9

Zaznacz tak, je ¶Æ• wszystkie punkty ko F6ðwe dost — æP dla klientów wymuszaj P TLS 1.2 lub wy Ç7§•. Preferowany jest TLS 1.3 Zwyk '' …EE Đusi przekierowywa r æ …EE 0.

MFA wymuszone dla wszystkich kont administracyjnych

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(j) / ENISA TIG §11.3

Zaznacz tak, je ¶Æ• ka ÆFP wewn —G'¦æP konto administracyjne na platformie SaaS musi u Ç—pa p MFA. Ten sam standard co Tw wewn —G'¦æ öÆ—G–¶ FÖ–æ—7G acyjna.

Docelowy czas przywrócenia (RTO) w godzinach

[integer] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(c) / ENISA TIG §4

Maksymalna liczba godzin, przez które Twoja us 'Vv mo ÆP by p niedost — æ przed przywróceniem. Realistyczna warto ± SLA, a nie warto ± docelowa. Typowe warto ¶6' 6 3 4, 8 lub 24 godziny.

4. Specyficzne dla On-Premise (4 pól)

Dostarczanie wykazu komponentów oprogramowania (SBOM)

[boolean] Warunkowe - Podstawa prawna: CRA / NIS2 Art. 21(2)(d)

Zaznacz tak, je ¶Æ• dostarczasz wykaz komponentów oprogramowania (SBOM) z ka ÆG–Đ wydaniem. CycloneDX lub SPDX to formaty standardowe. Obowi W¦°owe na mocy Cyber Resilience Act dla produktów wprowadzanych na rynek UE od grudnia 2027 r.

Wydania s R öG —6 æR · yptograficznie

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(e) / ENISA TIG §6.5

Zaznacz tak, je ¶Æ• ka ÆG• artefakt wydania ma podpis kryptograficzny, który klienci mog P zweryfikowa rà Klucze podpisuj V6P udokumentowane i podlegaj R &÷F 6¦'à Licz R 6' zarówno podpisy Sigstore, jak i PGP.

Opublikowana polityka ujawniania podatno ¶6•

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(e) / ENISA TIG §3

Zaznacz tak, je ¶Æ• masz publicznie udokumentowany sposób zg & 7¦ æ– podatno ¶6• bezpiecze G7Gpa. Wystarczy plik security.txt w Twojej domenie (zgodnie z RFC 9116) lub dedykowany adres e-mail, taki jak security@example.com.

SLA poprawek dla krytycznych CVE (godziny)

[integer] Warunkowe - Podstawa prawna: CIR 2024/2690 §5.1.4(f)

Godziny od publicznego ujawnienia CVE do wydania z poprawk P dla krytycznych podatno ¶6• (CVSS 9.0+). Realistyczne zobowi W¦ æ–P, a nie warto ± docelowa. Typowe warto ¶6" 24, 48 lub 72 godziny.

5. Professional Services (3 pól)

Zakres weryfikacji przesz &ñ[ci

[string] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(i) / CIR 2024/2690 §5.1.4(c)

Opisz, w jaki sposób weryfikujesz konsultantów do stanowisk wra ÆÆ—w–6,à Przyk & C wyci Vp z rejestru karnego dla wszystkich konsultantów oraz sprawdzenie referencji w przypadku zlece B ö&V¦Đuj V7–6, F æR æ–V¦ wne.

NDA zawarte ze wszystkimi konsultantami

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(i) / ENISA TIG §11.4

Zaznacz tak, je ¶Æ• ka ÆG• konsultant podpisuje umow • o zachowaniu poufno ¶6• przed przydzieleniem do pracy u klienta. Jako cz '[umowy o prac ' Æ&ò ¦ °o odr –&æR ä@A.

Udokumentowana polityka zachowania w siedzibie klienta

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Zaznacz tak, je ¶Æ• masz pisemny kodeks post — ðwania dla konsultantów pracuj V7–6€ w siedzibie klienta: obs 'Vv identyfikatorów, obowi W ek blokowania ekranu, post — ðwanie w przypadku wyniesienia danych z lokalizacji.

6. Managed Services (3 pól)

Wdro ÆöæR ¦ '¡ dzanie dost — VÒ W '§—v–ÆV¦ðwanym (PAM)

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(i) / ENISA TIG §11.3

Zaznacz tak, je ¶Æ• u Ç—pasz narz –G¦– do zarz VG¦ æ– dost — VĐ uprzywilejowanym dla administracyjnych sesji zdalnych w systemach klientów. Przyk & G" CyberArk, BeyondTrust, Teleport. Konfiguracja jump-host z rejestrowaniem logów si ' Æ–7§•.

Sesje administracyjne s R &V¦W7G owane

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(f) / ENISA TIG §10

Zaznacz tak, je ¶Æ• sesje administracyjne w systemach klientów s P rejestrowane i przechowywane do celów weryfikacji. Typowy okres przechowywania: od 90 dni do 1 roku. Niezb –FæR Fò &V°onstrukcji forensycznej po incydentach.

Dy ÇW" #Bóp

[boolean] Warunkowe - Podstawa prawna: NIS2 Art. 21(2)(b) / ENISA TIG §3

Zaznacz tak, je ¶Æ• prowadzisz dy ÇW 24/7, który reaguje na incydenty bezpiecze G7Gpa w systemach klientów. Wsparcie wy ! cznie w godzinach pracy nie spe &æ– FVvò w–ÖöwRà