

PLAN SZKOLEŃ

Planowany przebieg modułów szkoleniowych

KSC / NIS2 dla branży fotowoltaicznej — kadra zarządzająca i pracownicy

60 min łączy czas modułu	45 min treść, ćwiczenie i podsumowanie	15 min pytania uczestników
------------------------------------	--	--------------------------------------

Założenia organizacyjne

Format: każdy moduł trwa 60 minut: 45 minut części merytoryczno-warsztatowej oraz 15 minut pytań uczestników.

Ćwiczenia: są wliczone w część 45-minutową i powinny kończyć się krótkim omówieniem decyzji uczestników.

Podsumowania: zamykają moduł checklistą, pytaniami sprawdzającymi albo wskazaniem dalszych działań.

Walidacja: czasy są punktem wyjścia; przed wdrożeniem zalecana jest próba prowadzącego z rzeczywistymi materiałami.

Aktualność prawna: terminy, sankcje i przesłanki podlegania należy zweryfikować bezpośrednio przed każdym szkoleniem.

Dokument zawiera dziewięć harmonogramów: cztery dla kadry zarządzającej oraz pięć dla pracowników, ponieważ moduł dotyczący OT został rozpisany w wariantach ogólnym i technicznym.

1. Kadra zarządzająca

Moduł 1. Wstęp i samoidentyfikacja

Proponowany czas	Zakres
5 min	Otwarcie: cel modułu, skutki błędnej samoidentyfikacji i zebranie podstawowych informacji o uczestnikach oraz ich organizacjach.
8 min	Zasada samoidentyfikacji podmiotu i odpowiedzialność kierownictwa za prawidłową ocenę zakresu obowiązków.
10 min	Mapa ról w sektorze PV: wytwórca energii, agregator, operator magazynu, spółka projektowa, właściciel farmy, instalator i podmiot świadczący usługi.
7 min	Pułapki kwalifikacyjne: wielkość przedsiębiorstwa, struktury grupowe, SPV oraz dodatkowe przesłanki objęcia obowiązkami.
10 min	Ćwiczenie: przejście przez dwa przykładowe przypadki i przygotowanie wstępnej decyzji na podstawie właściwych załączników i danych organizacji.
5 min	Podsumowanie: checklista danych do samoidentyfikacji, wskazanie właściciela decyzji i dalszych kroków dokumentacyjnych.
15 min	Pytania uczestników i omówienie przypadków granicznych.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Uwaga: Bezpośrednio przed każdym szkoleniem zweryfikować aktualny stan prawny, terminy i brzmienie przesłanek.

Moduł 2. Odpowiedzialność kierownika podmiotu

Proponowany czas	Zakres
5 min	Otwarcie: czego kierownik nie może sprowadzić do „zadania działu IT” i jakie decyzje pozostają po stronie kierownictwa.
8 min	Zakres odpowiedzialności kierownika za realizację zadań cyberbezpieczeństwa oraz granice delegowania obowiązków.
5 min	Sankcje i środki nadzorcze jako kontekst odpowiedzialności, bez dominowania nad praktyczną częścią modułu.
10 min	Dowody wykonywania nadzoru: protokoły decyzji, raporty, akceptacje ryzyka, przeglądy, rejestry działań i potwierdzenia realizacji.
7 min	Kontrola zadań delegowanych: właściciel, termin, kryterium odbioru, częstotliwość raportowania, eskalacja i zamknięcie zadania.
7 min	Ćwiczenie: odpowiedzialność zarządu po incydencie wynikającym z błędu dostawcy lub niewykonania zadania przez dział IT.
3 min	Podsumowanie: pięć pytań kontrolnych, na które kierownik powinien umieć odpowiedzieć po szkoleniu.
15 min	Pytania uczestników i odniesienie zasad do ich modelu organizacyjnego.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Uwaga: Sankcje ograniczono do pięciominutowego kontekstu, a dodatkowy czas przeznaczono na dowody nadzoru i kontrolę zadań delegowanych.

Moduł 3. Ryzyko dostawcy i należyta staranność

Proponowany czas	Zakres
5 min	Otwarcie: dlaczego zależność od dostawcy jest ryzykiem biznesowym wymagającym decyzji kierownictwa.
6 min	Mapa kluczowych dostawców i zależności: usługi, procesy oraz skutki przerwania lub pogorszenia współpracy.
8 min	Kryteria należytej staranności przed wyborem dostawcy: kompetencje, zarządzanie bezpieczeństwem, historia incydentów, ciągłość działania, podwykonawcy i przedstawiane dowody.
7 min	Właściciel ryzyka: odpowiedzialność za ocenę, sposób postępowania z ryzykiem, akceptację decyzji i raportowanie do kierownictwa.
6 min	Nadzór w toku współpracy: wskaźniki, przeglądy, niezgodności, działania naprawcze i dokumentowanie oceny dostawcy.
5 min	Warunki zakończenia współpracy i plan wyjścia: przesłanki decyzji, zachowanie ciągłości, przekazanie informacji i odebranie dostępów.
5 min	Ćwiczenie: decyzja zarządcza na podstawie niepełnych dowodów dostawcy i powtarzających się uchybień.
3 min	Podsumowanie: checklista wyboru, nadzoru i zakończenia współpracy z dostawcą.
15 min	Pytania uczestników i omówienie stosowanych modeli współpracy z dostawcami.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Moduł 4. Łańcuch dostaw i gotowość organizacji

Proponowany czas	Zakres
5 min	Otwarcie: dlaczego odporność łańcucha dostaw wpływa na ciągłość działania i wiarygodność organizacji.
8 min	Kaskadowanie oczekiwań bezpieczeństwa w ekosystemie OSD, przemysłu, samorządu, wykonawców EPC, serwisu O&M i podwykonawców.
5 min	Rozporządzenie 2024/1366: orientacyjny kontekst i identyfikacja sytuacji, w których potrzebna jest odrębna analiza specjalistyczna.
7 min	Gotowość organizacji: procesy, odpowiedzialności i dowody, które pokazują zdolność do zarządzania cyberbezpieczeństwem.
7 min	Zgodność i dojrzałość jako element wiarygodności biznesowej oraz relacji z klientami i partnerami.
6 min	Harmonogram, budżet i kolejność prac: działania pilne, przygotowanie SZBI, audyt i rozwój nadzoru nad dostawcami.
4 min	Ćwiczenie: ustalenie priorytetów rocznego planu podnoszenia gotowości organizacji i łańcucha dostaw.
3 min	Podsumowanie: decyzje, właściciele i działania do podjęcia po szkoleniu.
15 min	Pytania uczestników dotyczące gotowości organizacji i zależności w łańcuchu dostaw.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

2. Pracownicy

Moduł 1. Phishing i socjotechnika w realiach branży PV

Proponowany czas	Zakres
5 min	Otwarcie: jak socjotechnika wykorzystuje rutynę, pośpiech, autorytet i chęć szybkiego załatwienia sprawy.
8 min	Najczęstsze scenariusze: fałszywa faktura, zmiana rachunku, wiadomość od zarządu, współdzielony plik, kod QR i telefon od rzekomego serwisu.
8 min	Sygnały ostrzegawcze: presja czasu, nietypowa domena, skrócony link, załącznik wymagający logowania, prośba o poufność lub kod MFA.
7 min	Bezpieczna weryfikacja: drugi kanał, znany numer, samodzielnie otwarty portal i zasada niewykonywania polecenia przed potwierdzeniem.
10 min	Ćwiczenie: analiza trzech wiadomości związanych z zakupem, serwisem i płatnością; decyzja: wykonuję, weryfikuję albo zgłaszam.
5 min	Omówienie ćwiczenia i powiązanie z modułem 4: co zrobić po kliknięciu lub przekazaniu danych.
2 min	Podsumowanie: trzy nawyki przed kliknięciem, zeskanowaniem kodu lub wykonaniem przelewu.
15 min	Pytania uczestników i omówienie wiadomości podobnych do spotykanych w pracy.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Moduł 2. Hasła, MFA i bezpieczna praca na urządzeniach

Proponowany czas	Zakres
5 min	Otwarcie: konto pracownika jako tożsamość w systemie i punkt wejścia do poczty, portali, monitoringu oraz usług serwisowych.
7 min	Indywidualne konta i rozliczalność: dlaczego nie współdzielimy loginów i jak odbiera się dostęp po zmianie roli.
8 min	Hasła i menedżer haseł: unikalność, bezpieczne przechowywanie i korzystanie wyłącznie z rozwiązań zatwierdzonych przez organizację.
8 min	MFA w praktyce: nieoczekiwane monity, wyłudzenie kodów, seria powiadomień i właściwa reakcja na podejrzenie przejęcia konta.
7 min	Bezpieczne urządzenie i praca mobilna: blokada ekranu, aktualizacje, zatwierdzone aplikacje, publiczne Wi-Fi, utrata lub kradzież sprzętu.
7 min	Ćwiczenie: reakcja na monit MFA, prośbę o udostępnienie loginu i utratę telefonu z dostępem do poczty służbowej.
3 min	Podsumowanie: checklista ochrony konta i urządzenia.
15 min	Pytania uczestników i omówienie zasad obowiązujących w ich organizacji.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Uwaga: Przed szkoleniem potwierdzić, jaki menedżer haseł, sposób MFA, proces utraty urządzenia i zasady pracy zdalnej są rzeczywiście zatwierdzone u klienta.

Moduł 3A. Świadomość OT dla wszystkich pracowników

Wariant ogólny — dla pracowników technicznych i nietechnicznych.

Proponowany czas	Zakres
5 min	Otwarcie: czym OT różni się od systemów biurowych i dlaczego błąd cyfrowy może oddziaływać na rzeczywistą instalację.
7 min	Mapa środowiska PV: urządzenia sterujące, portal monitoringu, chmura, konta dostawców, zdalny serwis i urządzenia używane do obsługi.
7 min	Punkty styku pracownika z OT: wiadomości serwisowe, raporty, faktury, zaproszenia do portali, prośby o dane i zatwierdzenie dostępu.
7 min	Socjotechnika „na serwisanta”: potwierdzenie osoby, firmy, zakresu prac i właściwego kanału kontaktu.
7 min	Zasady bezpiecznego zachowania: brak udostępniania kont, instalowania narzędzi i zatwierdzania dostępu poza uzgodnionym procesem.
8 min	Ćwiczenie: wiadomość od rzekomego serwisu, alarm w portalu i prośba o pilny dostęp — wykonuję, weryfikuję czy zgłaszam?
4 min	Podsumowanie: rola pracownika nietechnicznego i ścieżka zgłoszenia nietypowej sytuacji.
15 min	Pytania uczestników i omówienie ich kontaktów z portalami, dostawcami i serwisem.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Uwaga: Nie rozszerzać o szczegóły konfiguracji i narzędzia serwisowe. W materiałach używać prostego schematu instalacji oraz przykładów z codziennej pracy uczestników.

Moduł 3B. Bezpieczna praca serwisowa i dostęp do OT

Wariant techniczny — dla serwisu, O&M, automatyków, administratorów i osób organizujących dostęp dostawców.

Proponowany czas	Zakres
5 min	Otwarcie: priorytety IT i OT, zależności między urządzeniami oraz konsekwencje nieplanowanej zmiany.
7 min	Podłączanie laptopów, telefonów, pamięci USB i narzędzi diagnostycznych; zatwierdzony sprzęt i oprogramowanie.
8 min	Zdalny dostęp dostawcy: potwierdzenie tożsamości, okno prac, najmniejsze uprawnienia, rejestrowanie czynności i zamknięcie dostępu.
8 min	Zmiany konfiguracji i aktualizacje: zatwierdzony zakres, możliwość odtworzenia, plan wycofania, osoba decyzyjna i test po zmianie.
5 min	Dokumentowanie prac: kto, kiedy, na jakim urządzeniu, w jakim celu, co zmienił i jaki uzyskał wynik.
8 min	Ćwiczenie: pilna prośba serwisanta o instalację narzędzia z prywatnego linku i dostęp zdalny; decyzja i wymagane zabezpieczenia.
4 min	Podsumowanie: checklista przed pracą, w trakcie i po zakończeniu dostępu serwisowego.
15 min	Pytania uczestników i odniesienie programu do stosowanych narzędzi oraz procedur.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Uwaga: Przed szkoleniem zebrać procedury klienta dotyczące dostępu zdalnego, zmian, nośników i zgłoszeń.

Moduł 4. Rozpoznanie, zgłoszenie i pierwsza reakcja na incydent

Proponowany czas	Zakres
5 min	Otwarcie: rola pracownika — rozpoznać sygnał, bezpiecznie przerwać działanie i przekazać informację bez samodzielnej kwalifikacji prawnej.
8 min	Przykładowe sygnały: przejęte konto, złośliwy załącznik, utrata urządzenia, błędna wysyłka, ransomware, anomalia portalu lub niedostępność usługi.
7 min	Pierwsze działania i zakazy: zatrzymanie podejrzanej czynności, brak kolejnych zatwierdzeń, niekasowanie śladów i nieprowadzenie własnego dochodzenia.
5 min	Zachowanie informacji: czas, komunikat, nadawca lub adres strony, identyfikator urządzenia, wykonane czynności i bezpieczny zrzut ekranu.
5 min	Kanał główny i zapasowy oraz kompletne zgłoszenie: kto, kiedy, czego dotyczy, objawy, wpływ, działania i dane kontaktowe.
8 min	Ćwiczenie: dwa przypadki — kliknięty link i ujawnione hasło oraz nietypowa zmiana w portalu monitoringu; przygotowanie zgłoszenia.
7 min	Omówienie i podsumowanie: checklista pierwszych pięciu minut, współpraca po zgłoszeniu i użycie procesu zastępczego.
15 min	Pytania uczestników i omówienie sytuacji właściwych dla ich organizacji.
Razem: 60 min	45 min części merytoryczno-warsztatowej + 15 min pytań uczestników

Uwaga: Przed wdrożeniem szkolenia wstawić rzeczywiste kanały alarmowe, tryb zgłaszania poza godzinami pracy oraz zasady postępowania, gdy poczta lub system zgłoszeń nie działa.