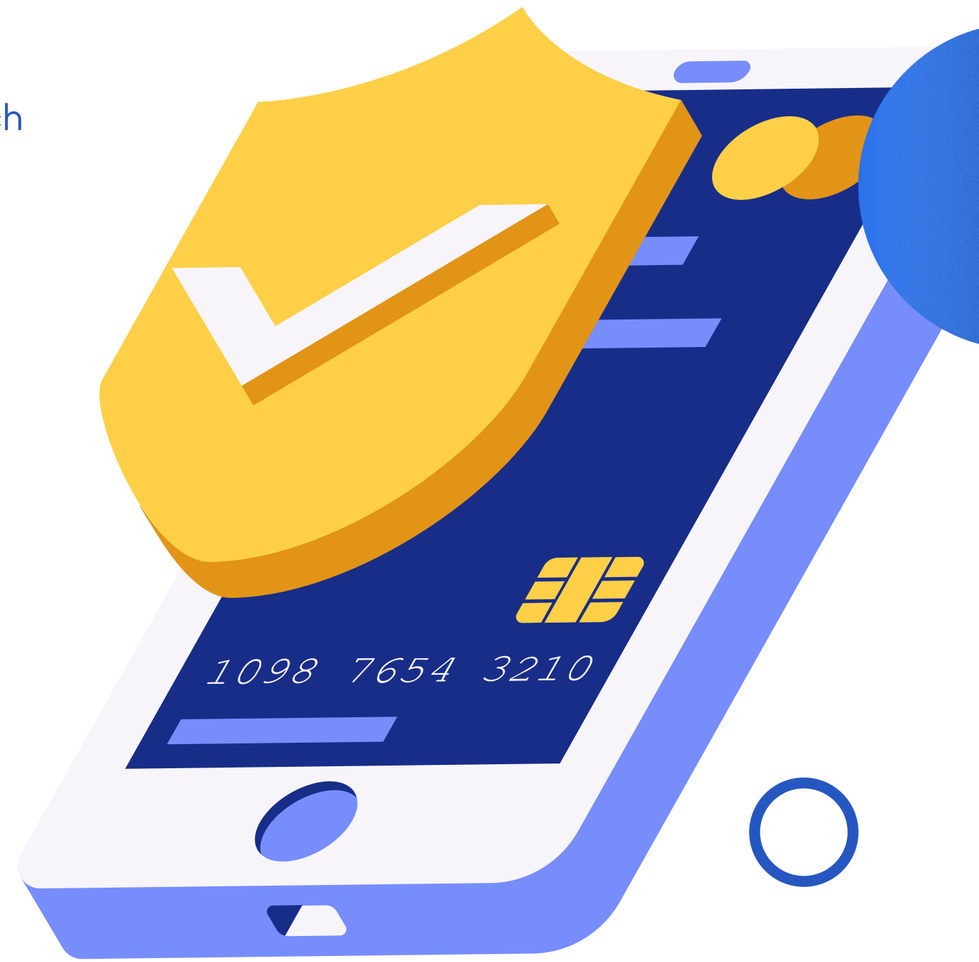
SZKOLENIE DLA DOSTAWCÓW EPEC

Bezpieczeństwo informacji i cyberbezpieczeństwo w relacjach z EPEC Sp. z o. o.

Elbląg, listopad 2025

Cel szkolenia

- Zrozumienie zasad bezpieczeństwa informacji i cyberbezpieczeństwa obowiązujących w EPEC.
- Poznanie wymagań formalnych przed rozpoczęciem współpracy.
- Świadomość odpowiedzialności za bezpieczeństwo danych i systemów IT/OT.



Ramy prawne i normatywne

- Dyrektywa NIS 2 (UE 2022/2555) – bezpieczeństwo w łańcuchu dostaw usług kluczowych.
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC).
- RODO – ochrona danych osobowych.
- ISO/IEC 27001 – A.15: bezpieczeństwo informacji w relacjach z dostawcami.
- Procedury EPEC:
- PS-P-02 – Zarządzanie i eksploatacja systemów IT,
- PS-P-07 – Bezpieczeństwo informacji w relacjach z dostawcami,
- PS-P-06 – Zarządzanie bezpieczeństwem osobowym,
- PS-I-06 – Zarządzanie bezpieczeństwem danych osobowych.

Kogo dotyczy szkolenie

Dostawcy, którzy:

- mają dostęp do systemów informatycznych, sieci lub infrastruktury IT/OT,
- przetwarzają lub utrzymują dane osobowe w imieniu EPEC,
- mają dostęp do informacji poufnych lub krytycznych,
- świadczą usługi o znaczeniu kluczowym (ERP, poczta, backup, SOC, bezpieczeństwo IT/OT),
- wykonują prace serwisowe, hostingowe lub zdalne,
- obsługują systemy bezpieczeństwa fizycznego/logicznego.

Zasada wspólnej odpowiedzialności

„Bezpieczeństwo EPEC zaczyna się od bezpieczeństwa dostawcy."

Każdy podmiot współpracujący z EPEC:

- odpowiada za ochronę informacji,
- działa zgodnie z zasadami SZBI,
- zgłasza incydenty i naruszenia,
- zapewnia zgodność z przepisami i umowami.

Proces kwalifikacji dostawcy

Etap 1: Inicjacja

1. Komórka merytoryczna zgłasza potrzebę współpracy.
2. Określa, czy dostawca będzie miał dostęp do:
    - danych osobowych, informacji poufnych lub krytycznych
    - systemów IT/OT,
    - infrastruktury lub usług kluczowych.

➡️ To decyduje, czy dostawca podlega pełnej kwalifikacji w ramach SZBI.

Etap 2: Klasyfikacja i ocena dostawcy

1. Dostawca wypełnia Ankietę PS-P-07-1.
2. Komórka EPEC dokonuje oceny wg Analizy PS-P-07-2:

- zgodność z ISO 27001 i RODO,
- mechanizmy bezpieczeństwa (dostęp, szyfrowanie, backup, incydenty),
- gotowość do testów/audytów.

3. Wynik:

- zaakceptowany,
- krytyczny dostawca → wpis na Listę PS-P-07-3,
- odrzucony – brak spełnienia wymagań SZBI.

Etap 3: Weryfikacja zgodności z RODO

Jeśli dostawca przetwarza dane osobowe:

- wypełnia Ankietę do umowy powierzenia PS-I-06-5,
- analizę zatwierdza Inspektor Ochrony Danych (IOD),
- zawiera się:
    - Umowę powierzenia PS-I-06-6, lub
    - Upoważnienie PS-I-06-1 (dla osób fizycznych).

Etap 4: Wymagane umowy i oświadczenia

Każdy dostawca podpisuje przed rozpoczęciem współpracy:

- Umowa NDA - zobowiązanie do ochrony informacji,
- Oświadczenie dostawcy o poufności - potwierdzenie znajomości zasad bezpieczeństwa,
- Umowa powierzenia / upoważnienie - gdy przetwarzane są dane osobowe
- Oświadczenia pracowników dostawcy - indywidualne potwierdzenie poufność i dostępu do danych osobowych

Proces kwalifikacji dostawcy

Etap 5: Szkolenie i nadanie dostępów

Każdy pracownik dostawcy z dostępem do systemów EPEC musi:

- odbyć szkolenie z zasad bezpieczeństwa informacji lub przedstawić potwierdzenie wcześniejszego szkolenia,
- dostępy nadawane są na wniosek + akceptacja ASI.

➡️ Bez potwierdzonego szkolenia – brak dostępu do środowiska EPEC.

Etap 6: Monitorowanie i nadzór

Krytyczni dostawcy – audyt co najmniej raz na 2 lata.
Wymagane raporty bezpieczeństwa / testy penetracyjne.
EPEC może przeprowadzić niezapowiedziany audyt.
Incydenty należy zgłosić nie później niż 2 h od wykrycia.

Etap 7: Reagowanie na incydenty

- Zgłoszenie niezwłocznie → e-mail + telefon do Zespołu ds. Cyberbezpieczeństwa.
- Raport końcowy w ciągu 24 h.
- Jeśli incydent dotyczy danych osobowych → EPEC zgłasza do UODO w 72 h.
- Współpraca z SOC EPEC i CSIRT NASK.

Przykłady: phishing, ransomware, wyciek danych, utrata nośnika, nieautoryzowany dostęp.

WYMAGANIA TECHNICZNE I ORGANIZACYJNE DLA DOSTAWCÓW EPEC

1. Ochrona dostępu i tożsamości

Uwierzytelnianie użytkowników

- Każdy użytkownik (pracownik dostawcy) posiada indywidualny identyfikator (login) — używanie wspólnych kont jest zabronione.
- Logowanie wymaga hasła spełniającego politykę EPEC:
  - Użytkownicy: min. 10 znaków, wielkie i małe litery, cyfry, znak specjalny.
  - Administratorzy: min. 14 znaków, większa złożoność.
  - Zmiana hasła: użytkownicy co 3 miesiące, administratorzy co 6 miesięcy.
  - Po 3 błędnych próbach — automatyczna blokada konta.
  - Nie wolno używać dat, imion, nazw, numerów telefonów itp.

Zarządzanie uprawnieniami

- Uprawnienia przyznaje się zgodnie z zasadą „need to know” — tylko do zasobów niezbędnych do realizacji umowy.
- Dostęp przyznawany jest na wniosek i usuwany na wniosek lub z upływem terminu obowiązywania.
- Dostawca zobowiązany jest prowadzić rejestr osób z dostępem i przekazywać go EPEC do zatwierdzenia.
- Dostępy są okresowo weryfikowane i audytowane.

WYMAGANIA TECHNICZNE I ORGANIZACYJNE DLA DOSTAWCÓW EPEC

2. Ochrona systemów informatycznych

Aktualizacje i utrzymanie systemów

- Wszystkie systemy IT i OT muszą być objęte procesem aktualizacji oprogramowania i łatek bezpieczeństwa — nie rzadziej niż raz w miesiącu.
- Niedozwolone jest używanie oprogramowania niezatwierdzonego przez EPEC.
- Zmiany i aktualizacje muszą być testowane przed wdrożeniem i rejestrowane w Dzienniku Administratora.

Zabezpieczenia przed malware i atakami

- Wszystkie urządzenia muszą mieć aktualne oprogramowanie antywirusowe.
- Wszelkie pliki z zewnątrz należy skanować przed użyciem.
- Zabronione jest instalowanie programów spoza oficjalnych źródeł.

Segmentacja i separacja sieci

- Sieć OT (technologiczna) musi być odseparowana od sieci IT (biurowej).
- Dostęp z zewnątrz (np. serwisowy) odbywa się wyłącznie przez bezpieczne łącza VPN z kontrolą tożsamości i rejestrowaniem sesji.

WYMAGANIA TECHNICZNE I ORGANIZACYJNE DLA DOSTAWCÓW EPEC

3. Ochrona danych i informacji

Szyfrowanie

- Dane wrażliwe, osobowe i poufne muszą być szyfrowane.
- Każdy nośnik danych opuszczający teren EPEC musi być zaszyfrowany i oznaczony.

Nośniki danych i Biała Lista

- Dozwolone są wyłącznie zatwierdzone pendrive'y / dyski znajdujące się na Białej Liście EPEC.
- Prywatne lub znalezione nośniki – bezwzględnie zakazane.
- Dane osobowe na nośnikach wymiennych — tylko w wyjątkowych, uzasadnionych przypadkach i muszą być natychmiast usuwane po wykorzystaniu.
- Nośniki z danymi osobowymi przechowywane są w zamykanych szafach lub sejfach.

Usuwanie i utylizacja nośników

- Dane należy usuwać metodą bezpiecznego nadpisywania lub demagnetyzacji.
- Zużyte nośniki przekazywane są do utylizacji firmie posiadającej odpowiednie certyfikaty lub niszczone w niszczarkach o odpowiedniej klasie (P-4 lub P-5).

WYMAGANIA TECHNICZNE I ORGANIZACYJNE DLA DOSTAWCÓW EPEC

4. Praca zdalna i urządzenia mobilne

Zasady pracy zdalnej

- Połączenia z siecią EPEC wyłącznie przez VPN z dwustopniowym uwierzytelnianiem.
- Zabronione korzystanie z otwartych sieci Wi-Fi.
- Użytkownik ma obowiązek blokować ekran podczas przerw w pracy.

Urządzenia mobilne

- Muszą mieć włączone szyfrowanie dysku, hasło lub PIN do logowania.
- Urządzenia mobilne OT nie mogą być używane w sieci IT ani w celach prywatnych.

5. Komunikacja elektroniczna i e-mail

Poczta służbowa

- Do kontaktu z EPEC używa się wyłącznie służbowych kont e-mail.
- Dane poufne lub osobowe muszą być zaszyfrowane lub zabezpieczone hasłem, przekazanym innym kanałem.
- Zabronione jest przesyłanie informacji służbowych z kont prywatnych.

Internet

- Internet służy wyłącznie do celów zawodowych związanych z realizacją umowy.
- Blokowane są strony o treściach niezgodnych z prawem lub polityką EPEC.
- Zabronione jest pobieranie oprogramowania z nieautoryzowanych źródeł.

WYMAGANIA TECHNICZNE I ORGANIZACYJNE DLA DOSTAWCÓW EPEC

6. Wymagania organizacyjne

- Dostawca wyznacza osobę odpowiedzialną za bezpieczeństwo informacji i kontakt z EPEC.
- Wszyscy pracownicy mający dostęp do informacji EPEC podpisują indywidualne oświadczenia o poufności.
- Dostawca zapewnia szkolenia dla swojego personelu w zakresie bezpieczeństwa.
- Zabronione jest przekazywanie danych lub zlecanie prac podwykonawcom bez pisemnej zgody EPEC.

7. Wymagania wobec sprzętu i infrastruktury

- Urządzenia muszą być objęte konserwacją i przeglądami technicznymi.
- Naprawy i serwisy mogą być wykonywane tylko przez autoryzowane podmioty.
- Przed naprawą należy usunąć lub zabezpieczyć dane znajdujące się na nośnikach.

8. Odpowiedzialność dostawcy

- Dostawca ponosi pełną odpowiedzialność za naruszenia wynikające z niedochowania zasad bezpieczeństwa.
- EPEC może zawiesić lub zakończyć współpracę w przypadku:
  - poważnego incydentu,
  - braku zgłoszenia incydentu,
  - nieprzestrzegania umów lub procedur.

Zarządzanie incydentami

- Każdy dostawca musi mieć wdrożone zasady zarządzania incydentami.
- Incydent należy zgłosić nie później niż w ciągu 2 godzin od wykrycia: mailowo do iod@epec.elblag.pl lub it@epec.elblag.pl
- Raport incydentu – w ciągu 24 godzin po zakończeniu jego obsługi.
- W przypadku naruszenia danych osobowych – EPEC zgłasza incydent do UODO w ciągu 72 godzin.

Podsumowanie

Wymagania techniczne i organizacyjne są nie tylko formalnością, lecz obowiązkiem wynikającym z:

- NIS 2,
- Ustawy o KSC,
- ISO 27001 (A.9, A.12, A.13, A.14, A.15, A.17),
- i wewnętrznych regulacji EPEC.

Ich celem jest utrzymanie ciągłości działania, ochrona danych, i zapewnienie cyberodporności całego łańcucha dostaw.

Dziękuję i zapraszam do kontaktu

+48 55 611 32 00

www.epec.pl

it@epec.elblag.pl

ul. Fabryczna 3, 82-300 Elbląg