

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przeprowadzenie audytu zgodności z wymogami Ustawy o krajowym systemie cyberbezpieczeństwa i Dyrektywy NIS2:

Przeprowadzenie audytu w formie wizji lokalnej posiadanych przez Zakład Komunikacji Miejskiej w Ciechanowie Spółka z o.o. środków technicznych i organizacyjnych polegającego m.in. na:

- a) przeglądzie obecnych polityk, procedur i środków bezpieczeństwa,
- b) identyfikacji systemów/aplikacji/usług IT i OT, kluczowych aplikacji oraz potencjalnych luk w zabezpieczeniach,
- c) analiza BIA (Business Impact Analysis), identyfikacja krytycznych zasobów (MAK),
- d) ocenie zgodności z aktualnymi przepisami i standardami cyberbezpieczeństwa
- e) przygotowaniu dokładnej listy z opisem wymagań, która Spółka musi spełnić by posiadać system zarządzania bezpieczeństwem informacji (system cyberbezpieczeństwa) wymagany przez ustawę o Krajowym Systemie Cyberbezpieczeństwa i NIS2 wraz z koncepcją wdrożenia przedmiotowego systemu.

Raport musi też zawierać kompleksową ocenę obecnego stanu bezpieczeństwa informacji w ZKM w Ciechanowie Spółka z o.o. oraz obecnych luk i braków wraz z rekomendacją sposobu ich usunięcia.

Audyt i raport musi być sporządzony zgodnie z Metodyką audytu (opisująca metodę przeprowadzenia audytu spełniająca wymogi ustawowe oraz norm i dobrych praktyk).

Audyt i raport musi być zrealizowany przez Zespół, w składzie którego co najmniej dwie osoby posiadają, co najmniej jeden z certyfikatów wskazanych poniżej, zgodnie z wymaganiami Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu:

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);
- Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 ze zm.), w zakresie certyfikacji osób;
- Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

2. Przeprowadzenia analizy ryzyk w ZKM w Ciechanowie Spółka z o.o. wymaganej od tzw. Podmiotów ważnych przez ustawę o Krajowym Systemie Cyberbezpieczeństwa i NIS2. Analiza



ryzyk musi uwzględniać m.in. wszystkie aktywa, podatności, zabezpieczenia i zagrożenia (zagrożenia bezpieczeństwa informacji lub ciągłości działalności), prawdopodobieństwa, potencjalne skutki itd. tak, by rzetelnie oszacować ryzyka wystąpienia incydentu oraz móc zarządzać tymi ryzykami.

Przedstawienie planów naprawczych w przypadku ryzyk oszacowanych na wysokie lub bardzo wysokie.

Analiza ryzyk musi być przeprowadzona zgodnie z Metodologią analizy ryzyk (opisującą metodę przeprowadzenia analizy ryzyk spełniającą wymogi ustawowe oraz norm i dobrych praktyk).

PREZES ZARZĄDU
[Signature]
Waldemar Kiciński
2.10.2026