MANOWIECKI
CYBERSECURITY LAW

KANCELARIA ADWOKACKA
ul. Wiosny Ludów 29 · 62-200 Gniezno
+48 694 715 335 · kancelaria@manowiecki.legal
www.manowiecki.legal

Czy Twoja organizacja jest gotowa na nowe wymogi cyberbezpieczeństwa?

Czy Twoje przedsiębiorstwo w myśl ustawy o krajowym systemie cyberbezpieczeństwa jest podmiotem kluczowym bądź ważnym:

1. Spełnia wymagania do uznania jako średni przedsiębiorca tj. zatrudnia co najmniej 250 pracowników i którego roczny obrót przekracza 50 milionów EURO, lub roczna suma bilansowa przekracza 43 miliony EURO?

   TAK ☐ NIE ☐

2. Należy do sektora? (np. Energetycznego, Transportowego, Finansowego, Ochrony Zdrowia, Infrastruktury cyfrowej, Zarządzania usługami technologi informacyjno-komunikacyjnych).

   TAK ☐ NIE ☐

3. Spełnia wymagania do uznania jako średni przedsiębiorca tj. zatrudnia co najmniej 50 pracowników i którego roczny obrót lub roczna suma bilansowa przekracza 10 milionów EURO?

   TAK ☐ NIE ☐

4. Należy do sektora? (np. Gospodarowania odpadami, Produkcji, wytwarzania i dystrybucji chemikaliów, Produkcji, przetwarzania i dystrybucji żywności, Produkcji, Dostawców usług cyfrowych, Badań naukowych).

   TAK ☐ NIE ☐

5. W praktyce organizacja zajmuje się?

   Odpowiedź:

   _____

MANOWIECKI
CYBERSECURITY LAW

KANCELARIA ADWOKACKA
ul. Wiosny Ludów 29 · 62-200 Gniezno
+48 694 715 335 · kancelaria@manowiecki.legal
www.manowiecki.legal

Czy w Twoim przedsiębiorstwie:

1. Występuje spisana i wdrożona polityka bezpieczeństwa informacji?
   TAK ☐ NIE ☐
2. Występuje spisana polityka szacowania ryzyka z zakresu bezpieczeństwa infomacji?
   TAK ☐ NIE ☐
3. Występuje spisana polityka wykonywania kopii zapasowych?
   TAK ☐ NIE ☐
4. Występuje spisana procedura pracy zdalnej i mobilnej?
   TAK ☐ NIE ☐
5. Stosuje się umowy o zachowaniu poufności?
   TAK ☐ NIE ☐
6. Występuje z góry ustalony proces bezpieczeństwa w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego?
   TAK ☐ NIE ☐
7. Występuje proces testowania wykorzystywanego systemu informacyjnego?
   TAK ☐ NIE ☐
8. Występuje proces bezpieczeństwa fizycznego i środowiskowego uwzględniający kontrole dostępu?
   TAK ☐ NIE ☐
9. Występuje proces ustalający zasady bezpieczeństwa wśród personelu?
   TAK ☐ NIE ☐
10. Występuje spisany proces bezpieczeństwa w relacji z dostawcą sprzętu lub oprogramowania IT?
    TAK ☐ NIE ☐
11. Występuje spisany proces zapewniania ciągłości działania wykorzystywanych systemów IT oraz OT?
    TAK ☐ NIE ☐

KANCELARIA ADWOKACKA
ul. Wiosny Ludów 29 · 62-200 Gniezno
+48 694 715 335 · kancelaria@manowiecki.legal
www.manowiecki.legal

12. Plany odtworzenia systemów po awarii są testowane w praktyce?

TAK ☐ NIE ☐

13. objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,

TAK ☐ NIE ☐

14. Występują polityki i procedury oceny skuteczności zastosowanych w celu zapewnienia środków technicznych i organizacyjnych dla bezpieczeństwa?

TAK ☐ NIE ☐

15. Zapewnia się szkolenia z zakresu cyberbezpieczeństwa dla personelu?

TAK ☐ NIE ☐

16. Zapewnia się dostęp do podstawowych zasad cyberhigieny?

TAK ☐ NIE ☐

17. Występują polityki i procedury stosowania kryptografii oraz szyfrowania?

TAK ☐ NIE ☐

18. Występują bezpieczne środki komunikacji elektronicznej, uwzględniające stosowanie uwierzytelniania wieloskładnikowego?

TAK ☐ NIE ☐

19. Występuje procedura zarządzania aktywami?

TAK ☐ NIE ☐

20. Występują polityki kontroli dostępu bezpieczeństwa?

TAK ☐ NIE ☐

21. Zapewnia się zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usług?

TAK ☐ NIE ☐

22. Występuje procedura zarządzania incydentami bezpieczeństwa?

TAK ☐ NIE ☐

KANCELARIA ADWOKACKA
ul. Wiosny Ludów 29 · 62-200 Gniezno
+48 694 715 335 · kancelaria@manowiecki.legal
www.manowiecki.legal

23. Stosuje się środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usług przez organizację? Jeśli tak, jaki są to środki?

TAK ☐ NIE ☐

Jeśli tak, jakie: _____

24. Stosuje się mechanizmy zapewniające poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym? Jeśli tak, jakie są to mechanizmy?

TAK ☐ NIE ☐

Jeśli tak, jakie: _____

25. Stosuje się regularne aktualizacje oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji?

TAK ☐ NIE ☐

26. Stosuje się ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym? Jeśli tak, jakie są to środki ochrony?

TAK ☐ NIE ☐

Jeśli tak, jakie: _____

27. Stosuje się niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń? Jeśli tak, kto to wykonuje?

TAK ☐ NIE ☐

Jeśli tak, kto: _____

28. Zapewnia się możliwość czasowego ograniczenia ruchu sieciowego przychodzącego do infrastruktury organizacji?

TAK ☐ NIE ☐

KANCELARIA ADWOKACKA
ul. Wiosny Ludów 29 · 62-200 Gniezno
+48 694 715 335 · kancelaria@manowiecki.legal
www.manowiecki.legal

29. Zapewnia się w razie konieczności możliwość minimalizacji skutków ograniczenia dostępności usług, z uwagi na podjęte działania czasowego ograniczenia ruchu sieciowego przychodzącego do infrastruktury organizacji?

TAK ☐ NIE ☐

30. Wykorzystuje się systemy sztucznej inteligencji (AI)?

TAK ☐ NIE ☐

31. Występuje wdrożona norma ISO 27001?

TAK ☐ NIE ☐

32. Występuje wdrożona norma ISO 22301?

TAK ☐ NIE ☐

adw. Oskar Manowiecki
ISO 27001 i 22301 Lead Auditor