

Celem audytu będzie wykazanie zmiany poziomu bezpieczeństwa teleinformatycznego, która nastąpiła po zrealizowaniu czynności mających na celu podniesienie poziomu bezpieczeństwa, w odniesieniu do stanu na dzień przeprowadzenia w formie ankiety w Systemie Statystyki Ochrony Zdrowia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy, co pozwoli na spełnienie warunku koniecznego do otrzymania dotacji z Narodowego Funduszu Zdrowia, o którym mowa w par. 3 ust. 2 Zarządzenia 68/2022/BBIICD Prezesa NFZ.

## **I. Etap I - Audyt wstępny**

### **1. Cel Etapu I**

Zebranie, agregacja, analiza i ocena stanu rzeczywistego bezpieczeństwa systemów informacyjnych w placówce.

### **2. Produkt Etapu I - Raport z audytu wstępnego**

zawierający ocenę aktualnego na dzień podpisania umowy z wykonawcą poziomu bezpieczeństwa systemów informacyjnych oraz stanu posiadania przez placówkę dokumentacji w zakresie obowiązujących uregulowań.

### **3. Minimalny zakres Raportu z audytu wstępnego to opis:**

- 3.1. zidentyfikowanych systemów informacyjnych
- 3.2. organizacji wewnętrznej struktury cyberbezpieczeństwa
- 3.3. sposobu szacowania ryzyka dla systemu informacyjnego
- 3.4. organizacji systemu zarządzania bezpieczeństwem informacji (ISO 27001)
- 3.5. stosowanych zabezpieczeń systemu zarządzania bezpieczeństwem informacji (ISO 27001) (Załącznik A)
- 3.6. organizacji zarządzania ciągłością działania (ISO 22301):
- 3.7. sposobu zbierania informacji o zagrożeniach dla systemów informacyjnych i ich podatnościach
- 3.8. monitorowania systemu informacyjnego
- 3.9. sposobu zabezpieczenia dokumentacji dotyczącej cyberbezpieczeństwa
- 3.10. sposobu zarządzania incydentami
- 3.11. stosowanych sposobów:
  - 3.11.1. analizy kodu złośliwego
  - 3.11.2. badania odporności systemu informacyjnego
  - 3.11.3. zabezpieczenia śladów kryminalistycznych
- 3.12. stosowanych modeli oraz środków łączności wewnętrznej i zewnętrznej,
- 3.13. stosowanych zabezpieczeń przed utratą i kradzieżą danych
- 3.14. stosowanych sposobów kontroli dostępu do systemów informatycznych, w tym dostępu przez usługi zdalne
- 3.15. procedur i środków technicznych stosowanych dla zabezpieczeń przy pracy zdalnej
- 3.16. technicznej infrastruktury w systemach ICT, schematu sieci, a także zabezpieczeń sieci.
- 3.17. procedur i środków technicznych stosowanych dla zabezpieczeń dostępu do sieci publicznej
- 3.18. procedur i środków technicznych stosowanych dla zabezpieczeń wewnętrznej sieci ICT
- 3.19. systemu identyfikowania i uwierzytelniania użytkowników i administratorów
- 3.20. procedur i środków technicznych stosowanych dla backupów i archiwizacji danych, w tym testów odtworzeniowych,
- 3.21. zidentyfikowanych pojedynczych punktów awarii

- 3.22. procedur i środków technicznych stosowanych dla zapewnienia ciągłości pracy systemów i sieci
- 3.23. stosowanych systemów zabezpieczeń kryptograficznych
- 3.24. sposobu szyfrowania danych przechowywanych poza siedzibami Zamawiającego, w tym serwisy pocztowe email, serwisy WEB itp.
- 3.25. zabezpieczeń komputerów przed atakami phishingowymi
- 3.26. systemów ochrony poczty email i usług WEB pod kątem ataków phishingowych
- 3.27. procedur i środków technicznych stosowanych dla ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacji zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
- 3.28. procedur i środków technicznych stosowanych dla zapisów historii zmian w dokumentach, systemach informatycznych itp.
- 3.29. procedur i środków technicznych stosowanych dla zarządzania i zabezpieczania nośników przechowujących dane
- 3.30. zasad odpowiedzialności użytkowników
- 3.31. zasad zarządzania hasłami
- 3.32. procedur i środków technicznych stosowanych przy niszczeniu niepotrzebnych nośników i danych
- 3.33. sposobu zbierania logów, zakresu i retencji logów
- 3.34. zaangażowania kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji.

## **II. Etap II - Audyt systemu zarządzania bezpieczeństwem**

1. Warunek konieczny - zakończenie przez placówkę czynności podnoszących poziom bezpieczeństwa.
2. Cel Etapu II  
Celem audytu systemu zarządzania bezpieczeństwem jest wykazanie poziomu bezpieczeństwa teleinformatycznego w placówce, po zrealizowaniu czynności podnoszących poziom bezpieczeństwa, w szczególności w odniesieniu do poziomu bezpieczeństwa zdiagnozowanego na dzień sporządzenia Audytu wstępnego.
3. Produkt Etapu II - **Raport z audytu systemu zarządzania bezpieczeństwem**  
zawierający ocenę aktualnego na dzień sporządzenia raportu stanu bezpieczeństwa systemów informacyjnych oraz stanu posiadania przez Zamawiającego dokumentacji w zakresie obowiązujących uregulowań. Minimalny zakres Raportu z audytu systemu zarządzania bezpieczeństwem to opis:
  - 3.1. zidentyfikowanych systemów informacyjnych
  - 3.2. organizacji wewnętrznej struktury cyberbezpieczeństwa
  - 3.3. sposobu szacowania ryzyka dla systemu informacyjnego
  - 3.4. organizacji systemu zarządzania bezpieczeństwem informacji (ISO 27001)
  - 3.5. stosowanych zabezpieczeń systemu zarządzania bezpieczeństwem informacji (ISO 27001) (Załącznik A)
  - 3.6. organizacji zarządzania ciągłością działania (ISO 22301):
  - 3.7. sposobu zbierania informacji o zagrożeniach dla systemów informacyjnych i ich podatnościach
  - 3.8. monitorowania systemu informacyjnego
  - 3.9. sposobu zabezpieczenia dokumentacji dotyczącej cyberbezpieczeństwa
  - 3.10. sposobu zarządzania incydentami
  - 3.11. stosowanych sposobów:

- 3.11.1. analizy kodu złośliwego
- 3.11.2. badania odporności systemu informacyjnego
- 3.11.3. zabezpieczenia śladów kryminalistycznych
- 3.12. stosowanych modeli oraz środków łączności wewnętrznej i zewnętrznej,
- 3.13. stosowanych zabezpieczeń przed utratą i kradzieżą danych
- 3.14. stosowanych sposobów kontroli dostępu do systemów informatycznych, w tym dostępu przez usługi zdalne
- 3.15. procedur i środków technicznych stosowanych dla zabezpieczeń przy pracy zdalnej
- 3.16. technicznej infrastruktury w systemach ICT, schematu sieci, a także zabezpieczeń sieci.
- 3.17. procedur i środków technicznych stosowanych dla zabezpieczeń dostępu do sieci publicznej
- 3.18. procedur i środków technicznych stosowanych dla zabezpieczeń wewnętrznej sieci ICT
- 3.19. systemu identyfikowania i uwierzytelniania użytkowników i administratorów
- 3.20. procedur i środków technicznych stosowanych dla backupów i archiwizacji danych, w tym testów odtworzeniowych,
- 3.21. zidentyfikowanych pojedynczych punktów awarii
- 3.22. procedur i środków technicznych stosowanych dla zapewnienia ciągłości pracy systemów i sieci
- 3.23. stosowanych systemów zabezpieczeń kryptograficznych
- 3.24. sposobu szyfrowania danych przechowywanych poza siedzibami Zamawiającego, w tym serwisy pocztowe email, serwisy WEB itp.
- 3.25. zabezpieczeń komputerów przed atakami phishingowymi
- 3.26. systemów ochrony poczty email i usług WEB pod kątem ataków phishingowych
- 3.27. procedur i środków technicznych stosowanych dla ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacji zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
- 3.28. procedur i środków technicznych stosowanych dla zapisów historii zmian w dokumentach, systemach informatycznych itp.
- 3.29. procedur i środków technicznych stosowanych dla zarządzania i zabezpieczania nośników przechowujących dane
- 3.30. zasad odpowiedzialności użytkowników
- 3.31. zasad zarządzania hasłami
- 3.32. procedur i środków technicznych stosowanych przy niszczeniu niepotrzebnych nośników i danych
- 3.33. sposobu zbierania logów, zakresu i retencji logów
- 3.34. zaangażowania kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji.

### **III. Etap III - Audyt zmiany poziomu cyberbezpieczeństwa**

- 1. Warunek konieczny:
  - 1.1. zakończenie przez placówkę czynności podnoszących poziom bezpieczeństwa.
  - 1.2. zakończenie prac Etapu II oraz dostarczenie wykonawcy ankiety wypełnionej w Systemie Statystyki Ochrony Zdrowia badanie poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy
- 2. Cel Etapu III  
Celem Audytu zmiany poziomu cyberbezpieczeństwa jest wykazanie zmian poziomu bezpieczeństwa teleinformatycznego w placówce, po zrealizowaniu czynności podnoszących poziom bezpieczeństwa,

w odniesieniu do poziomu bezpieczeństwa zdiagnozowanego na dzień na dzień przeprowadzenia badania w formie ankiety w Systemie Statystyki Ochrony Zdrowia.

3. **Produkt Etapu III- Raport z audytu zmiany poziomu cyberbezpieczeństwa**

zawierający opis zmiany poziom bezpieczeństwa systemów informacyjnych, która nastąpiła po zrealizowaniu czynności mających na celu podniesienie poziomu bezpieczeństwa u świadczeniodawcy, w odniesieniu do stanu na dzień przeprowadzenia w formie ankiety w Systemie Statystyki Ochrony Zdrowia badania poziomu dojrzałości cyberbezpieczeństwa. Minimalny zakres Raportu z audytu zmiany poziomu cyberbezpieczeństwa to opis dokumentujący zmiany w następujących obszarach

3.1. Skuteczność działania infrastruktury

- 3.1.1. Urządzenia i konfiguracja w zakresie ochrony poczty
- 3.1.2. Urządzenia i konfiguracja w zakresie ochrony sieci
- 3.1.3. Urządzenia i konfiguracja w zakresie systemów serwerowych
- 3.1.4. Urządzenia i konfiguracja w zakresie stacji roboczych
- 3.1.5. Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa

3.2. Procesy zarządzania bezpieczeństwem informacji

- 3.2.1. Nośniki wymienne - udokumentowany sposób postępowania
- 3.2.2. Zarządzanie tożsamością / dostęp do systemów w zakresie:
- 3.2.3. Przydzielanie dostępu
- 3.2.4. Odbieranie dostępu
- 3.2.5. Pomieszczenia w dyspozycji zespołu odpowiedzialnego za cyberbezpieczeństwo, w przypadku podmiotów, które otrzymały decyzję uznającą podmiot za operatora usługi kluczowej.

3.3. Monitorowanie i reagowanie na incydenty bezpieczeństwa

- 3.3.1. Procedury zarządzania incydentami
- 3.3.2. Raportowanie poziomów pokrycia scenariuszami znanych incydentów
- 3.3.3. Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa
- 3.3.4. Monitorowanie i wykrycie incydentów bezpieczeństwa
- 3.3.5. Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów

3.4. Zarządzanie ciągłością działania

- 3.4.1. Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa
- 3.4.2. Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa
- 3.4.3. Procedury wykonywania i przechowywania kopii zapasowych
- 3.4.4. Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP)
- 3.4.5. Procedury utrzymaniowe

3.5. Utrzymanie systemów informacyjnych

- 3.5.1. Harmonogramy skanowania podatności
- 3.5.2. Aktualny status realizacji postępowania z podatnościami
- 3.5.3. Procedury związane ze z identyfikowaniem (wykryciem) podatności
- 3.5.4. Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami

3.6. Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług

- 3.6.1. Polityka bezpieczeństwa w relacjach z dostawcami
- 3.6.2. Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa
- 3.6.3. Dostęp zdalny
- 3.6.4. Metody uwierzytelnienia