Wojewódzki
Szpital Specjalistyczny
w Białej Podlaskiej

RFC 2350

Metryka dokumentu:

Tytuł	RFC 2350 WSzS w Białej Podlaskiej
Data wydania pierwszej wersji	14.04.2023
Data wygaśnięcia dokumentu	Dokument jest obowiązujący do czasu wydania kolejnej jego wersji
Właściciel	Wojewódzki Szpital Specjalistyczny w Białej Podlaskiej
Obecna wersja	1.0
Data publikacji obecnej wersji	14.04.2023

1. Informacje o dokumencie

Dokument zawiera opis Zespołu ds. Cyberbezpieczeństwa w Wojewódzkim Szpitalu Specjalistycznym w Białej Podlaskiej zgodnie z RFC 2350 oraz dostarcza podstawowych informacji o Zespole, sposobach kontaktu, opisuje zadania Zespołu i oferowane usługi.

1.1. Data ostatniej aktualizacji

Jest to wersja 1.0, wydana 14.04.2023 r.

1.2. Lista dystrybucyjna powiadomień o zmianach w dokumencie

Zespół ds. Cyberbezpieczeństwa w Wojewódzkim Szpitalu Specjalistycznym w Białej Podlaskiej nie korzysta z żadnej listy dystrybucyjnej mającej na celu powiadamianie o zmianach w tym dokumencie.

1.3. Lokalizacje, w których można znaleźć dokument

Aktualna wersja dokumentu dostępna jest pod linkiem:
https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

1.4. Uwierzytelnianie dokumentu

Niniejszy dokument został podpisany przy pomocy klucza PGP Wojewódzkiego Szpitala Specjalistycznego w Białej Podlaskiej. Jego sygnatura dostępna jest pod linkiem:
https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

2. Informacje kontaktowe

2.1. Nazwa Zespołu

Zespół ds. Cyberbezpieczeństwa

2.2. Adres

Zespół ds. Cyberbezpieczeństwa
Wojewódzki Szpital Specjalistyczny w Białej Podlaskiej
ul. Terebelska 57-65

21-500 Biała Podlaska

Polska

2.3. Strefa czasowa

Środkowoeuropejski (GMT+0100, GMT+0200 od kwietnia do października)

2.4. Numer telefonu

83 41 47 200

2.5. Telefaks numer

Niedostępny

2.6. Adres poczty elektronicznej

Wszystkie incydenty powinny być raportowane na adres mailowy:

cyberbezpieczenstwo@szpitalbp.pl

2.7. Inne możliwości komunikacji

Niedostępne

2.8. Klucze publiczne i inne informacje o szyfrowaniu

Zespół ds. Cyberbezpieczeństwa korzysta z klucza PGP

Email: cyberbezpieczenstwo@szpitalbp.pl

Klucz publiczny dostępny jest pod linkiem:

https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

2.9. Członkowie Zespołu

W skład Zespołu ds. Cyberbezpieczeństwa wchodzą eksperci w zakresie zagadnień dotyczących: cyberbezpieczeństwa, bezpieczeństwa środowiskowego oraz bezpieczeństwa fizycznego.

2.10. Inne informacje

Ogólne informacje na temat Wojewódzkiego Szpitala Specjalistycznego oraz na temat cyberbezpieczeństwa są dostępne pod linkiem:

https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

2.11. Punkty kontaktu z klientem

Zespół ds. Cyberbezpieczeństwa preferuje kontakt poprzez pocztę elektroniczną (e-mail) z wykorzystaniem kluczy kryptograficznych w celu zapewnienia integralności i poufności komunikacji.

W sprawach ogólnych: kontakt możliwy jest od 7.30 do 15.05 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

Zgłoszenia incydentów, sytuacje kryzysowe: kontakt telefoniczny z Zespołem ds. Cyberbezpieczeństwa i/lub wiadomość e-mail zawierająca szczegóły podane telefonicznie.

Telefon Zespołu ds. Cyberbezpieczeństwa jest dostępny w godzinach pracy od 7.30 do 15.05 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

3. Statut

3.1. Misja

Misją Zespołu ds. Cyberbezpieczeństwa jest budowanie kompetencji i zdolności pacjentów oraz pracowników w identyfikowaniu, zapobieganiu i podejmowaniu działań minimalizujących prawdopodobieństwo wystąpienia incydentów cyberbezpieczeństwa, jak również niwelujących skutków ich wystąpienia (w zakresie świadczonych usług).

3.2. Zakres działania

Zespół ds. Cyberbezpieczeństwa zapewnia wsparcie w zakresie obsługi zdarzeń bezpieczeństwa w cyberprzestrzeni dla swoich pacjentów, pracowników i klientów.

3.3. Finansowanie i przynależność

Nadzór nad działalnością Wojewódzkiego Szpitala Specjalistycznego w Białej Podlaskiej sprawuje Zarząd Województwa Lubelskiego. Wojewódzki Szpital

Specjalistyczny w Białej Podlaskiej prowadzi gospodarkę finansową na zasadach określonych w obowiązujących przepisach prawa polskiego.

3.4. Umocowanie

Organem założycielskim Wojewódzkiego Szpitala Specjalistycznego w Białej Podlaskiej jest Samorząd Województwa Lubelskiego.

4. Zasady obsługi incydentów (polityki)

4.1. Rodzaje incydentów i poziom wsparcia

Priorytet normalny jest domyślnym priorytetem wszystkich rodzajów incydentów związanych z cyberbezpieczeństwem mogących wystąpić w środowisku teleinformatycznym w zakresie świadczonych usług.

Sposób obsługi incydentów przez Zespół ds. Cyberbezpieczeństwa zależy od rodzaju i wagi incydentu lub zdarzenia, elementów, na które oddziałuje incydent, ilości użytkowników, których dotyczy incydent oraz dostępności zasobów Zespołu ds. Cyberbezpieczeństwa w tym czasie. Dla zdarzeń określa się priorytety stosownie do ich dotkliwości i rozmiaru.

Incydenty obsługiwane dobrowolnie, w interesie publicznym mają zatem normalny priorytet bez względu na oznaczenie dołączone do powiadomienia o zdarzeniu. O podniesieniu priorytetu decyduje każdorazowo Zespół ds. Cyberbezpieczeństwa.

4.2. Współpraca, interakcja i ujawnianie informacji

Zespół ds. Cyberbezpieczeństwa oświadcza, że wszystkie informacje dotyczące obsługi incydentów są rozpatrywane jako poufne.

Zespół ds. Cyberbezpieczeństwa wymienia wszystkie niezbędne do współpracy informacje z innymi zespołami CSIRT, a także z administratorami zainteresowanych stron. Żadne dane osobowe nie są wymieniane, chyba że za wyraźnym upoważnieniem. Wszystkie informacje związane z obsługiwanymi incydentami są traktowane jako chronione. Informacje chronione (takie jak dane osobowe, konfiguracje systemu, znane luki, etc.) są szyfrowane, jeśli muszą być przesyłane w niezabezpieczonym środowisku.

Informacje przesyłane do Zespołu ds. Cyberbezpieczeństwa mogą być przekazywane zgodnie z potrzebą stronom zaufanym (takim jak dostawcy usług internetowych, inne zespoły CERT) wyłącznie w celu obsługi incydentów.

4.3. Komunikacja i uwierzytelnianie

Zespół ds. Cyberbezpieczeństwa wykorzystuje szyfrowanie w celu zapewnienia poufności i integralności komunikacji. Wszystkie wrażliwe informacje, które są przesyłane, powinny być szyfrowane.

Dane o niskiej wrażliwości można wysyłać za pomocą niezaszyfrowanych wiadomości e-mail, jednak nie jest to uznawane za bezpieczne. Zalecane jest szyfrowanie PGP, szczególnie w przypadku poufnych danych.

Zespół ds. Cyberbezpieczeństwa zastrzega sobie prawo do weryfikacji autentyczności informacji lub jej źródła w zakresie dozwolonym przez prawo.

5. Usługi

5.1. Reakcja na incydenty

Wojewódzki Szpital Specjalistyczny w Białej Podlaskiej ustanowił organizacyjny i techniczny proces reagowania na incydenty. Proces obejmuje pełny cykl reagowania na incydenty:

- obsługę,
- zarządzanie,
- rozwiązywanie,
- łagodzenie

5.2. Prewencja

Zespół ds. Cyberbezpieczeństwa prowadzi działania mające na celu zwiększenie odporności środowiska informatycznego na zdarzenia związane z cyberbezpieczeństwem i minimalizujące potencjalny wpływ tych zdarzeń.

6. Formularze zgłaszania incydentów

Nie ma specjalnych formularzy zgłaszania incydentów do Zespołu ds. Cyberbezpieczeństwa.

7. Zastrzeżenia

Podczas przygotowywania informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności.

Zespół ds. Cyberbezpieczeństwa nie ponosi odpowiedzialności za błędy, pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.