CSIRT Wielospecjalistyczny Szpital - Samodzielny Publiczny Zespół Opieki Zdrowotnej w Zgorzelcu CERT (wersja polska)

1. Informacje o dokumencie

Dokument zawiera opis zespołu CERT w Wielospecjalistycznym Szpitalu - Samodzielnym Publicznym Zespole Opieki Zdrowotnej w Zgorzelcu zgodnie z RFC 2350 oraz dostarcza podstawowych informacji o CERT, sposobach kontaktu, opisuje obowiązki zespołu i oferowane usługi.

1.1 Data ostatniej aktualizacji

Wersja dokumentu 1.00, opublikowana 27.04.2023.

1.2 Lista dystrybucyjna powiadomień o zmianach w dokumencie

CERT w Wielospecjalistycznym Szpitalu - Samodzielnym Publicznym Zespole Opieki Zdrowotnej w Zgorzelcu nie korzysta z żadnej listy dystrybucyjnej mającej na celu powiadamianie o zmianach w tym dokumencie.

1.3 Miejsce, w którym można znaleźć dokument

Aktualna wersja tego dokumentu znajduje się na:
https://www.spzoz.zgorzelec/index.php/rodo/cyberbezpieczenstwo

1.4 Wiarygodność dokumentu

Niniejszy dokument został podpisany przy użyciu klucza PGP Wielospecjalistycznego Szpitala - Samodzielnego Publicznego Zespołu Opieki Zdrowotnej w Zgorzelcu CERT. Więcej szczegółów w rozdziale 2.8.

2. Informacje kontaktowe

2.1 Nazwa zespołu

"Wielospecjalistyczny Szpital - Samodzielny Publiczny Zespół Opieki Zdrowotnej CERT ":
Zespół ds. Reagowania na incydenty cyberbezpieczeństwa - nazywany dalej jako Zespół ds. Zarządzania Bezpieczeństwem Informacji

2.2 Adres

Zespół ds. Zarządzania Bezpieczeństwem Informacji
Wielospecjalistyczny Szpital - Samodzielny Publiczny Zespół Opieki Zdrowotnej w Zgorzelcu ul. Lubańska 11-12, 59-900 Zgorzelec, Polska

2.3 Strefa czasowa

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

2.4 Numer telefonu

608359043 lub 571334972

2.5 Telefaks Numer

Niedostępny

2.6 Inne możliwości komunikacji

Niedostępne

2.7 Elektroniczny adres e-mail

cyberbezpieczenstwo@spzoz.zgorzelec.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu

Zespół ds. Zarządzania Bezpieczeństwem Informacji korzysta z klucza PGP:
Nazwa: WS-SPZOZ w Zgorzelcu Zespół ds. Zarządzania Bezpieczeństwem Informacji
Email: cyberbezpieczenstwo@spzoz.zgorzelec.pl
Identyfikator klucza:ECE27B76
Rozmiar klucza: 4096
Algorytm: RSA

Klucz ten można otrzymać bezpośrednio z naszej strony internetowej:
https://www.spzoz.zgorzelec.pl/index.php/rodo/cyberbezpieczenstwo

2.9 Członkowie zespołu

Zespół ds. Zarządzania Bezpieczeństwem Informacji składa się z ekspertów w dziedzinie zagadnień Cyberbezpieczeństwa.

2.10 Inne informacje

Ogólne informacje na temat Wielospecjalistycznego Szpitala - Samodzielnego Publicznego Zespołu Opieki Zdrowotnej w Zgorzelcu są zamieszczone na stronie internetowej https://www.spzoz.zgorzelec.pl/index.php

2.11 Punkty kontaktu z klientem

Zespół ds. Zarządzania Bezpieczeństwem Informacji preferuje kontakt mailowy.
Użyj powyższego klucza kryptograficznego, aby zapewnić integralność i poufność komunikacji.
W sprawach ogólnych:
Kontakt jest możliwy w godzinach pracy: 07:30-15:00 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

Zgłoszenia incydentów, sytuacje awaryjne:
Kontakt telefoniczny z Zespołem ds. Zarządzania Bezpieczeństwem Informacji oraz / lub wiadomość e-mail zawierająca szczegóły podane telefonicznie.
Telefon Zespołu ds. Zarządzania Bezpieczeństwem Informacji jest dostępny w godzinach pracy: 07:30-15:00 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

3. Statut

3.1 Misja

Budowanie kompetencji i zdolności Wielospecjalistycznego Szpitala - Samodzielnego Publicznego Zespołu Opieki Zdrowotnej w Zgorzelcu w zakresie unikania, identyfikowania i ograniczania cyberzagrożeń.
Wsparcie dla działań krajowych w zakresie bezpieczeństwa cybernetycznego.

3.2 Zakres działania

Zespół ds. Zarządzania Bezpieczeństwem Informacji zapewnia wsparcie w zakresie obsługi zdarzeń cyberbezpieczeństwa dla swoich pacjentów i klientów.

3.3 Finansowanie i przynależność

Nadzór nad działalnością Szpitala sprawuje Starostwo Powiatowe w Zgorzelcu.
Szpital prowadzi gospodarkę finansową na zasadach określonych w obowiązujących przepisach prawa polskiego.

3.4 Umocowanie

Organem założycielskim i sprawującym nadzór nad Szpitalem jest Starosta Powiatowy w Zgorzelcu.

4. Zasady obsługi incydentów (polityki)

4.1 Rodzaje incydentów i poziom wsparcia

Zespół ds. Zarządzania Bezpieczeństwem Informacji jest dedykowany do obsługi wszystkich rodzajów incydentów związanych z bezpieczeństwem komputerowym, które występują lub mogą wystąpić w środowisku teleinformatycznym Szpitala.
Klasyfikacja incydentów i sposób ich obsługi są określone w procesie zarządzania incydentami bezpieczeństwa informacji.
Sposób obsługi incydentów zależy od rodzaju i wagi incydentu lub zdarzenia, elementów, na które oddziałuje incydent, ilości użytkowników, których dotyczy incydent oraz dostępności zasobów. Dla zdarzeń określa się priorytety stosownie do ich dotkliwości i rozmiaru.

4.2 Współpraca, interakcja i ujawnianie informacji

Zespół ds. Zarządzania Bezpieczeństwem Informacji 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. Zarządzania Bezpieczeństwem Informacji 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. Zarządzania Bezpieczeństwem Informacji wykorzystuje szyfrowanie w celu zapewnienia poufności i integralności komunikacji. Wszystkie przesyłane informacje chronione powinny być szyfrowane.

5. Usługi

5.1 Reakcja na incydenty

Szpital ustanowił organizacyjny i techniczny proces reagowania na incydenty. Proces obejmuje pełny cykl reagowania na incydenty:

- obsługę
- zarzadzanie
- rozwiazywanie
- łagodzenie

5.1.1 Ocena incydentów

Ocena incydentów obejmuje

- analizę wpływu incydentu na bezpieczeństwo informacji przetwarzanych w Szpitalu
- nadawanie priorytetu stosownie do rodzaju i wagi incydentu
- określenie zakres incydentu
- przeprowadzenie badania przyczyn powstania incydentu

5.1.2 Koordynacja incydentów

Za koordynowanie działań odpowiada Przewodniczący Zespołu ds. Zarządzania Bezpieczeństwem Informacji w tym m.in.:

- ułatwianie kontaktu z innymi stronami, które mogą być zaangażowane
- kontakt z CSIRT NASK i/lub w razie potrzeby z odpowiednimi organami ścigania
- tworzenie raportów dla innych CSIRT

5.1.3 Rozwiązywanie incydentów

Obejmuje:

- powiadamianie zespołu i koordynację odpowiednich działań
- śledzenie postępów prac zaangażowanego zespołu
- obsługę żądań raportowania
- przedstawianie raportów

5.2 Działania proaktywne

Zespół ds. Zarządzania Bezpieczeństwem Informacji prowadzi działania mające na celu zwiększenie odporności środowiska informatycznego na zdarzenia związane z bezpieczeństwem i minimalizujące potencjalny wpływ tych zdarzeń.

6. Formularze zgłaszania incydentów

Wspomniany powyżej proces zarządzania incydentami bezpieczeństwa informacji definiuje mailowy (cyberbezpieczenstwo@spzoz.zgorzelec.pl) kanał zgłaszania incydentów.

W zgłoszenia incydentu prosimy o przekazanie do Zespołu ds. Zarządzania Bezpieczeństwem Informacji co najmniej następujących informacji:

- dane kontaktowe i informacje organizacyjne: imię i nazwisko, nazwa organizacji i adres, adres e-mail, numer telefonu oraz wszelkie istotne elementy techniczne i obserwacje
- adresy IP lub nazwę domenową (jeśli istnieją)

- wyniki skanowania (jeśli istnieją)
- wyciąg z rejestru log systemu (jeśli istnieją)

7. Zastrzeżenia

Podczas przygotowywania informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności.
Zespół ds. Zarządzania Bezpieczeństwem Informacji nie ponosi odpowiedzialności za błędy, pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.