gmina@inowlodz.pl

Od:
Wysłano: piątek, 10 lutego 2023 10:03
Do: gmina@inowlodz.pl
Temat: Re: RE: Nie udzielona odpowiedź na zapytanie z informacji publicznej

Korzystając z przysługujących mi praw oraz w trosce o wysoki poziom cyberbezpieczeństwa na terenie województwa łódzkiego na podstawie art. 61 Konstytucji RP oraz art. 10 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej wnoszę o udostępnienie następującej informacji:

1. **Czy system zarządzania bezpieczeństwem informacji w Twojej organizacji uwzględnia sformalizowane procedury?**

1. Tak
2. Nie

2. **Czy w podmiocie był przeprowadzany audyt z KRIO: zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r. poz. 526) zgodnie z § 20 ust.2 pkt 14) KRI?**

1. Tak
2 Nie

3. **Czy podmiot dysponuje całościową Polityką Bezpieczeństwa Informacji, wymaganą w §20 ust. 1 i 3 ww. Rozporządzenia oraz polityki ochrony danych, rejestrów czynności, analiz ryzyka wraz z procedurami? Jeśli odpowiedź jest twierdząca - wnosimy o krótkie - w kilku ogólnych zdaniach - opisanie przedmiotowej polityki oraz procedur?**

1. Tak
2. Nie
3. .....

4. **Czy zgodnie z art. 20 ust. 2 pkt 14 KRI (Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych) realizują Państwo w jednostce okresowy (nie rzadziej niż raz na rok) audyt wewnętrzny w zakresie bezpieczeństwa informacji?**

1. Tak
2. Nie

5. **Jeśli tak to proszę o wskazanie:**

1. terminu wykonania ostatniego audytu KRI

.....

1. w jaki sposób udokumentowany jest audyt

.....

6. **Czy zgodnie z wymogiem art. 20 ust. 1 ww. Rozporządzenia Państwa jednostka opracowała i ustanowiła, wdrożyła i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność?**

1. Tak
2. Nie

7. **Czy zarządzanie bezpieczeństwem informacji w Państwa jednostce prowadzone jest poprzez realizację i egzekwowanie działań wskazanych w art. 20 ust. 2 ww. Rozporządzenia?**

1. Tak
2. Nie

8. **Czy zapewniono aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia?**

1. Tak
2. Nie

9. **Czy utrzymywana jest aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację?**

1. Tak
2. Nie

10. **Czy przeprowadzono okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji? oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy?**

1. Tak
2. Nie

11. **Czy podejmowano działania minimalizujące ww. ryzyko, stosownie do wyników przeprowadzonej analizy?**

1. Tak
2. Nie
3. Nie dotyczy

12. **Czy osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji?**

1. Tak
2. Nie

13. **Czy dokonywana jest bezzwłoczna zmiana uprawnień, w przypadku zmiany zadań osób, które posiadają dostępy do systemów informatycznych?**

1. Tak
2. Nie

14. **Czy przeprowadzane są szkolenia osób zaangażowanych w proces przetwarzania informacji i użytkowników systemów informatycznych ze szczególnym uwzględnieniem takich zagadnień, jak:**

- Zagrożenia bezpieczeństwa informacji:

1. Tak
2. Nie

- Skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna:

1. Tak
2. Nie

3) Stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich:

1. Tak
2. Nie

15. **Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:**

- Monitorowanie dostępu do informacji:

1. Tak
2. Nie

- Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji:

1. Tak
2. Nie

3) Zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji:

1. Tak
2. Nie
3. **Czy ustanowiono podstawowe zasad gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość?**

1. Tak
2. Nie

17. **Czy zabezpieczono informacje w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie?**

1. Tak
2. Nie

18. **Czy zawierano umowy serwisowe podpisane ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji?**

1. Tak
2. Nie

19. **Czy ustalono zasady postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych?**

1. Tak
2. Nie

20. **Czy zapewniono odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:**

- Dbałości o aktualizację oprogramowania:

1. Tak
2. Nie

2) Minimalizowaniu ryzyka utraty informacji w wyniku awarii:

1. Tak
2. Nie

3) Ochronie przed błędami, utratą, nieuprawnioną modyfikacją:

1. Tak
2. Nie

4) Stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa:

1. Tak
2. Nie

5) Zapewnieniu bezpieczeństwa plików systemowych:

1. Tak
2. Nie

6) Redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

1. Tak
2. Nie

7) Niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa:

1. Tak
2. Nie

- Kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa:

1. Tak
2. Nie

- Bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących?

1. Tak
2. Nie

21. **Czy zapewniono okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok:**

1. Tak
2. Nie

22. **Czy macie Państwo wyznaczoną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa zgodnie z wymogiem art. 21 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa?**

1. Tak
2. Nie

23. **Czy osoba jest zgłoszona do CERT koordynator ds. cyberbezpieczeństwa?**

1. Tak
2. Nie

24. **Czy, zgodnie z art. 22 ust. 1 pkt 5 ww. ustawy dane tej osoby zostały przekazane do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV?**

1. Tak
2. Nie

25. **Jakie ta osoba posiada doświadczenie i kwalifikacje?**

1. posiada wykształcenie z zakresu cyberbezpieczeństwa
2. wykształcenie informatyczne jeśli tak to jakie .....
3. inne .....(proszę wpisać)

26. **W jaki sposób w Państwa jednostce zapewnione jest zarządzanie incydentem?**

(proszę opisać)

.....

27. **Czy Państwa jednostka zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej?**

1. Tak
2. Nie

28. **Proszę o wskazania ilości incydentów w zakresie cyberbezpieczeństwa od dnia 05.07.2018 roku.**

.....

29. **Proszę wskazać rodzaj zdarzenia, które spowodowało incydent (proszę zaznaczyć właściwe):**
30. atak phishingowy
31. atak ransomvare
32. błąd ludzki
33. wirus
34. trojan
35. brak aktualizacji oprogramowania
36. zamierzone działanie pracownika/byłego pracownika
37. skanowanie
38. botnet
39. podatność
40. inny .....(proszę wpisać)
41. **Proszę o wskazania ilości incydentów naruszenia bezpieczeństwa zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (proszę zaznaczyć właściwe):**
42. a) atak phishingowy
43. b) atak ransomvare
44. c) błąd ludzki
45. d) wirus
46. e) trojan
47. f) brak aktualizacji oprogramowania
48. g) zamierzone działanie pracownika/byłego pracownika
49. h) skanowanie
50. i) botnet
51. k) podatność
52. h) inny .....(proszę wpisać)

31. **Czy w Państwa jednostce przyjęta została procedura szacowania ryzyka z zakresu cyberbezpieczeństwa?**
32. Tak
33. Nie

32. **Czy sporządzono analizę ryzyka z zakresu cyberbezpieczeństwa obejmującą integralność, dostępność, poufność, autentyczność:**
33. Tak
34. Nie

33. **Proszę o podanie daty przeprowadzonej analizy ryzyka zakresu cyberbezpieczeństwa obejmującą integralność, dostępność, poufność, autentyczność?**

.....

34. **Proszę wskazać w jakiej formie została sporządzona analiza ryzyka.**

.....

W dniu 2023-02-10 10:02:40 użytkownik gmina@inowlodz.pl napisał:

> Dzień dobry,
>
> bardzo proszę o podanie adresu e-mail z którego wspomniany WOUIP został złożony. Niestety pod wskazaną datą na naszej skrzynce odbiorczej nie odnotowaliśmy wiadomości spełniającej powyższe kryteria.
>
> Pozdrawiam
>
> Małgorzata Miszczyk
>
> Punkt Obsługi Interesanta
>
> 
>
> Urząd Gminy Inowłódz
>
> ul. Spalska 2
>
> 44 710-12-33 w. 12
>
> Klauzula RODO
>
> https://bip.inowlodz.pl/index.php?option=com_attachments&task=download&id=5664

From:
Sent: Friday, February 10, 2023 8:54 AM
Subject: Nie udzielona odpowiedź na zapytanie z informacji publicznej
Importance: High

Szanowni Państwo.

W następstwie nie rozpatrzenia wniosku o udostępnienie informacji z dnia 21.01.2023 roku proszę o wskazanie przyczyn nie udzielenie odpowiedzi ponieważ nie otrzymałem:

– powiadomienia związanego z brakiem realizacji zakresu podmiotowego lub przedmiotowego trybu wnioskowego udostępnienia informacji publicznej;

– informacji w postaci zanonimizowanej albo niezanonimizowanej;

– decyzji o odmowie udostępnienia informacji publicznej (w tym informacji przetworzonej);

Nadmieniam, że odmowa udostępnienia informacji publicznej (w tym informacji przetworzonej) następuje w formie decyzji administracyjnej, do której w świetle art. 16 i 17 u.d.i.p. mają zastosowanie przepisy kodeksu postępowania administracyjnego, w takim wypadku stronie służy odwołanie od decyzji (odpowiednio wniosek o ponowne rozpatrzenie sprawy), jak również skarga (sprzeciw) do sądu administracyjnego.