MIEJSKO - GMINNY
OŚRODEK POMOCY SPOŁECZNEJ
W BODZANOWIE
ul. Bankowa 7, 09-470 Bodzanów
NIP 774-25-75-774 REGON 610089316
tel. (24) 260 70 06 wew. 131, 143, 144

Bodzanów 17.10.2024r.

MGOPS/1239../2024

Pani Monika Majecka
monika.majecka99@o2.pl

Odpowiedź na wniosek o informację publiczną

1. Czy na stronie www są pełne danych IOD?
Ad. 1 Tak na stronie internetowej są udostępnione dane IOD.

2. Wnosimy o dokumentację potwierdzająca realizację zadań przez IOD lub opis jego działań od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO

Ad. 2. Odnosząc się do udostępnienia dokumentacji potwierdzającą realizację zadań przez IOD informuję iż dokumenty te mają charakter wewnętrzny- organizacyjny i porządkowy i nie mogą być udostępnione w trybie ustawy o dostępie do informacji publicznej. Zgodnie z wyrokiem **NSA z 4.04.2019 r.**, I **OSK 1709/17** uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych - nie stanowi informacji publicznej.

3. Czy zostały opracowane i wdrożone przepisy wewnętrzne, procedury, instrukcje i inne dokumenty dotyczące przetwarzania danych osobowych oraz bezpieczeństwa informacji. Jeśli tak to jakie?

Ad. 3 *Tak zostały wdrożone dokumenty:*

- *Polityka Ochrony danych Osobowych u Administratora*
- *Polityka Kluczy u Administratora*
- *Polityka Czystego Ekranu u Administratora*
- *Polityka Czystego Biurka u Administratora*
- *Procedury z Zakresu Ochrony Danych Osobowych*
- *Procedura Zarządzania Incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem*
- *Polityka Bezpieczeństwa Informacji*

4. Wnosimy o przedłożenie dokumentu potwierdzającego zapoznanie się pracowników z treścią obowiązujących przepisów wewnętrznych, ewentualnie wskazanie w jaki sposób zostali oni zapoznani.

Ad, 4

Pracownicy potwierdzali zapoznanie się z przepisami wewnętrznymi (imię, nazwisko, data i podpis)

Szczegóły tych dokumentów mają charakter wewnętrzny - organizacyjny i porządkowy i nie mogą być udostępnione w trybie ustawy o dostępie do informacji publicznej. Patrz pkt 2

5. Informacje dotyczące szkoleń pracowników w zakresie ochrony danych osobowych

przeprowadzanych po 25 maja 2018 roku (informacje tj. data szkolenia, zakres szkolenia, osoba prowadząca, listy obecności, czas trwania).

Ad. 5 *Szkolenia odbyły się 24.10.2023r. I 25.10.2023 r. przez Firmę EX LEGE SZKOLENIA PRAWNICZE, OUTSOURCING USŁUG IOD RAFAŁ ANDRZEJEWSKI z zakresu RODO BEZPIECZEŃSTWO INFORMACJI Z ELEMENTAMI CYBERBEZPIECZEŃSTWA. Listy obecności mają charakter wewnętrzny - organizacyjny i porządkowy i nie mogą być udostępnione w trybie ustawy o dostępie do informacji publicznej. Patrz pkt 2*

6. Czy został opracowany Rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

Ad. 6 *Tak został opracowany Rejestr czynności przetwarzania danych osobowych oraz jego zmiany.*

7. Czy został opracowany Rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany?

Ad. 7 *Tak został opracowany rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.*

8. W jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne

Ad. 8 *Obowiązek informacyjny jest realizowany poprzez dołączanie klauzuli RODO do wypełnianych wniosków, wysyłanie dokumentów wraz z klauzulą*

Obowiązujące klauzule znajdują się na stronie:

https://gopsbodzanow.bipstrona.pl/cms/12313/klauzule_informacyjne

9. W jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne.

Ad. 9 *Obowiązek informacyjny zrealizowano poprzez przygotowanie klauzul informacyjnych – poprzez pozyskiwanie danych z innych źródeł niż osoba , której dane dotyczą*

https://gopsbodzanow.bipstrona.pl/cms/12313/klauzule_informacyjne

10. Wnosimy o regulacje dotyczące monitoringu wizyjnego (jeśli jest). Procedura i Regulamin w tym zakresie.

Ad.10. Ośrodek nie posiada monitoringu wizyjnego

11. Czy IOD w ramach monitorowania przeprowadza regularne i systematyczne sprawdzenia/audyty w zakresie prawidłowości przetwarzania danych osobowych oraz przestrzegania rozporządzenia RODO, ustawy o.d.o. oraz regulacji wewnętrznych? Dokumentacja w tym zakresie (plany, sprawozdania, raporty, itp.).

Ad. 11 IOD przeprowadza protokół z czynności sprawdzających w zakresie ochrony danych osobowych oraz posiada audyt bezpieczeństwa informacji. Dokumentacja w tym zakresie ma charakter wewnętrzny i nie może być udostępniona w trybie ustawy o dostępie do informacji publicznej. Patrz pkt 2

12. W trybie dostępu do informacji publicznej – zwracamy się z prośbą o informację, czy w związku z monitoringiem wizyjnym miejsc publicznych prowadzonym przez Państwa jednostkę była prowadzona była ocena skutków w rozumieniu art. 35 ust. 1 rodo stosownie do treści tego przepisu:

Ad.12. Tut. Ośrodek nie posiada monitoringu wizyjnego.

13. Mając na uwadze powyższe wnosimy o informację czy została opracowana polityka retencji danych? Jakich czynności ona dotyczy?

Ad.13. Ośrodek nie posiada polityki retencji danych.

1.1) Na mocy art. 61 Konstytucji RP, w trybie inter alia: art. 6 ust. 1 pkt 3 lit. f, art. 6 ust. 1 pkt 5 Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10)

Wnosimy o udzielnie informacji publicznej w przedmiocie :

Wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej?

Odp. IOD nie posiada kwalifikacji w zakresie wiedzy prawniczej.

Czy IOD jest prawnikiem? Jakie posiada doświadczenie?

Odp. Nie IOD nie jest prawnikiem i nie posiada doświadczenia prawniczego.

Kto i w jaki sposób weryfikował kwalifikacje IOD?

Odp. *Weryfikacji kandydata na inspektora ochrony danych dokonał Administrator na podstawie nabytych kwalifikacji i doświadczenia zawodowego przez pracownika.*

W jaki sposób odbywają się systematyczne szkolenia pracowników prowadzone przez IOD. Proszę wskazać, kiedy miały one miejsce oraz zakres szkolenia – pomijając ogólny instruktaż i zapoznanie się z przepisami dot. ochrony danych.

Odp. Systematyczne szkolenia odbywają się w formie e-learning. Firma EX LEGE SZKOLENIA PRAWNICZE, OUTSOURCING USŁUG IOD RAFAŁ ANDRZEJEWSKI przesyła na adres e-mail link do szkolenia wraz z materiałami. IOD przesyła link każdemu pracownikowi który po zapoznaniu się z materiałami wykonuje test. Prawidłowo wykonany test kończy się certyfikatem. Ostatnie szkolenia miały miejsce 24 i 25.10.2023 z zakresu RODO Bezpieczeństwo Informacji Z Elementami Cyberbezpieczeństwa.

Czy na bieżąco przekazywane są IOD do akceptacji pod względem prawidłowości w zakresie ochrony danych osobowych projekty dokumentów tj. projekty umów, informacji udostępnianych w Biuletynie Informacji Publicznych, projekty przepisów wewnętrznych związanych z udostępnianiem bądź pozyskiwaniem danych osobowych.

Odp IOD sprawdza dokumentację pod względem prawidłowości w zakresie ochrony danych osobowych.

Pozostałe pytania:

1. Czy podmiot prowadzi BIP i pod jakim adresem internetowym

Ad. 1 Podmiot prowadzi BIP pod adresem: https://gopsbodzanow.bipstrona.pl

1. Z usług jakiego dostawcy BIP podmiot korzysta. Czy jest to www.nbip.pl lub

www.bip.edu.pl czy inny (podać jaki)?

Ad. 1 Podmiot korzysta z usług dostawcy tj. IDcom Group Sp. z o.o. Jest to Biuletyn Informacji Publicznej (Gov.pl/bip)

1. Jakie są umowne okresy świadczenia tej usługi. Jaka jest wartość umów brutto w poszczególnych okresach? Dane odrębnie za poszczególne okresy w latach 2017-do czerwca 2024.

Ad. 1 *Umowa Nr IDC/2017/5512 z dnia 30 stycznia 2017r.*

§6 pkt 1 Umowa jest zawarta na czas określony

§6 pkt 2 umowa wchodzi w życie w dniu 30 stycznia 2017r.

§6 pkt 4 okres rozliczeniowy umowy to 12 miesięcy

§6 pkt 5 usługi o których mowa w par. 1 są wykonywane w momencie rozpoczęcia każdego okresu rozliczeniowego.

Wartość umów brutto:

2018r. - 2022r. W kwocie 307,50zł

2023r.- 2024r. W kwocie 799,50 zł

1. Proszę podać liczbę informacji publicznych opublikowanych w BIP w latach 2017-do czerwca 2024r.

   Ad. 1 Nie zostały opublikowane żadne informacje na stronie BIP

1Proszę podać liczbę wniosków o informację publiczną jakie wpłynęły do podmiotu, liczbę wniosków na które udzielono odpowiedzi wraz wnioskowaną informacją, liczbę wniosków na które udzielono odpowiedzi odmownej udzielenia informacji, liczbę wniosków na które nie udzielono odpowiedzi, liczbę postępowań sądowych w związku wnioskami o informację publiczną. Jeśli sąd określił, że podmiot pozostawał w bezczynności podać ile razy to określił i w poszczególnych latach Dane odrębnie za rok 2017, 2018, 2019, 2020, 2021, 2022, 2023.

Ad. 1 Obecny Kierownik jednostki pełni funkcję od 01.08.2022r. Od tego czasu wpłynął jeden wniosek o udzielenie informacji publicznej na który została udzielona odpowiedź. Od 2017r. Do 31 lipca 2022r. brak jest dokumentacji w podanym zakresie.

4. Wnosimy o udostępnienie informacji publicznej w zakresie ilości dni urlopu wypoczynkowego pozostałych do wykorzystania kierownikowi jednostki oraz poszczególnym zastępcom (jeśli są)a także, czy w tym roku którejś z tych osób został lub zostanie wypłacony ekwiwalent za niewykorzystany urlop (jeśli tak w jakiej kwocie i komu)

Ad. 4 *Kierownik MGOPS – 17 dni urlopu*
Zastępca MGOPS – 42 dni urlopu (niewykorzystane 16 dni z ubiegłego roku jest spowodowana długotrwałą usprawiedliwioną nieobecnością pracownika.
Żadnej z w/w osób w tym roku nie został i nie zostanie wypłacony ekwiwalent za niewykorzystany urlop.

PYTANIA Z KRAJOWYCH RAM INTEROPERACYJNOŚCI

1. Kto dokonuje corocznych audytów z KRI?

Ad. 1 Audyt z KRI wykonała firma EX LEGE Szkolenia Prawnicze Outsourcing Usług IOD Rafał Andrzejewski

2. Czy IOD realizuje zadania w związku z KRIO?

Ad. 2 *Tak*

3. Kto przeprowadza audyt bezpieczeństwa?

Ad. 3 *Audyt z bezpieczeństwa wykonała firma EX LEGE Szkolenia Prawnicze Outsourcing Usług IOD Rafał Andrzejewski*

Pytania informacja publiczna:

Lp.	Zagadnienie	*Tak*	Nie	Uwagi
	Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.			
1.	Czy prowadzona jest ewidencja:	TAK		
	a) sprzętu informatycznego w ramach ewidencji majątkowej?CZY IOD KONTROLUJĘ EWIDENCJĘ	TAK		
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	TAK		
	c) umów serwisowych?	TAK		
2.	Czy przypisano konkretnym osobom obowiązki w zakresie prowadzenia powyższych ewidencji - w tym oprogramowania i nośników oprogramowania? Jeśli TAK proszę o przedłożenie dokumentu. CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W	TAK		Zarządzenie nr 7/2024 z dnia 10 stycznia 2024r. W sprawie wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
3.	Czy posiadam zinwentaryzowany sprzęt / oprogramowanie wraz z określeniem ważności danego komponentu dla całej jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	TAK		Dokument wewnętrzny
	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami			

4.	powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ		NIE	
5.	Czy pracownicy mogą podłączać swój sprzęt (laptopy, telefony, tablety) do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		NIE	
6.	Czy zapisuję każdy fakt podłączenia zewnętrznego sprzętu do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		NIE	Brak przypadków podłączenia własnego sprzętu do infrastruktury służbowej
7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		NIE	Brak podłączenia pod infrastrukturę służbową

Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

1.	Czy znam najistotniejsze zagrożenia dla zinwentaryzowanych systemów IT? *Jeśli TAK proszę o ich wskazanie*	Tak		-Kradzież danych - utrata integralności, dostępności lub poufności informacji
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	TAK		Internet
	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w		NIE	

3.	odpowiednim czasie? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*				
4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?	TAK			
5.	Czy znam potencjalne zagrożenia dla systemów, które znajdują się w mojej infrastrukturze lub w infrastrukturze zewnętrznej (outsourcing)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		NIE		

Podejmowanie działań zapewniających, że 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 wraz z bezzwłoczną zmianą uprawnień, w przypadku zmiany zadań.

1.	Czy wskazana/e jest/są w jednostce osoba/y odpowiedzialna/e za bezpieczeństwo IT w jednostce? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W* Jeśli TAK proszę o przedłożenie dokumentu.	Tak			
2.	Czy osoby te posiadają stosowne kompetencje? Jeśli TAK proszę o potwierdzenie tego faktu.	TAK			
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?	TAK			
	Czy uprawnienia, o których mowa w pkt 3 uprawniają jedynie do przetwarzania informacji w stopniu adekwatnym do realizowanych zadań?	TAK			

4.	*CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?		NIE	
6.	Czy na bieżąco aktualizowane są uprawnienia do dostępu (np. w momencie zmiany zakresu obowiązków)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	TAK		
7.	Czy prowadzona jest formalna listę zadań /obowiązków /uprawnień takich osób? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	TAK		

Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.				
	Należy zaznaczyć stosowane w jednostce rozwiązania.			
1.	Bieżące czynności monitorowania dostępu w tym logi (serwery, systemy, urządzenia sieciowe).	TAK		Dostęp do sieci i systemu jest za pomocą loginów i haseł
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:		NIE	
a.	ochrona sieci na poziomie portów LAN		NIE	
b.	BIOS		NIE	
	centralny system kontroli dostępu logicznego do			

c.	pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows		NIE	
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		NIE	
e.	system ochrony zewnętrznej klasy firewall		NIE	
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;		NIE	
g.	stosowanie tokenów z hasłami jednorazowymi		NIE	

Podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE PRACĘ NA ODLEGŁOŚĆ CZY TYLKO PRZEDSTAWIA DOKUMENTY*

1.	Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość? *Jeśli TAK proszę o przedłożenie dokumentu*		NIE	
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? Jeśli TAK proszę o udokumentowanie.		NIE	
3.	Czy w pracy na odległość stosuję bezpieczne metody połączenia?		NIE	

4.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?	TAK		
5.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)? Jeśli TAK proszę wskazać, w jaki sposób.		NIE	

Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*

1.	Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w umowach zawieranych z dostawcami sprzętu/ oprogramowania? Jeśli TAK proszę o udokumentowanie.	TAK		Umowy przetwarzania danych osobowych
2.	Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system)?		NIE	

Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?*

1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? Jeśli TAK proszę o przedłożenie.		NIE	
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?		NIE	
	Czy istniej możliwość zdalnego, trwałego		NIE	

3.	usunięcia danych z tego typu urządzenia?			
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?		NIE	
5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?		NIE	
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?		NIE	

Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.
CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. ANALIZA RYZYKA W/W

1.	Czy realizuję bieżące aktualizacje zarówno na stacjach PC (system operacyjny / java / adobe reader / flash itp.), jak i serwerach?	TAK		
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?		NIE	
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?	TAK		
4.	Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej / serwera po wykryciu na nim wirusa?		NIE	
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?	TAK		
6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?	TAK		
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?	TAK		

8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?		NIE	
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?	TAK		
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?		NIE	
11	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?	TAK		
12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?		NIE	
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?	TAK		
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)	TAK		

Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.				
1.	Czy istnieją w jednostce procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	TAK		
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?		NIE	

Czy jedynym kryterium wyboru dla IOD i innych usług bezpieczeństwa informacji niezależnie od formy świadczenia tych usługi jest cena?
Odp. Nie dotyczy ponieważ IOD jest pracownikiem jednostki.
Jeśli tak to prosimy o wyjaśnienie czy w związku z tym oznacza to, że ochrona informacji ma niski priorytet w zarządzaniu Państwa organizacją? Jeśli nie, to jakie inne kryteria Państwo stosujecie i z jaką wagą. Prosimy o uszczegółowienie tej kwestii.

Odp. Nie dotyczy

Czy Państwa jednostka organizacyjna wdrożyła wewnętrzną procedurę schematów podatkowych (MDR – Mandatory Disclosure Rules), zgodnie z wymaganiami ustawy ordynacja podatkowa ?

Odp. Nie dotyczy – Nie jesteśmy płatnikiem podatku VAT.

Odpowiedzi w ustawowym terminie tj. do 14 dni proszę kierować na adres poczty elektronicznej:

Odpowiedzi proszę przesłać na maila: monika.majecka99@o2.pl

KIEROWNIK
Miejsko-Gminnego Ośrodka Pomocy Społecznej
w Bodzanowie
mgr Mirosława Zagłewska