OCENA ZGODNOŚCI Z KRI*/ UoKSC**

Zasady oceny

Każdemu z zagadnień (opisywanych wymagań), w polu oznaczonym na żółto, należy przypisać ocenę wg poniższej skali:

0	Brak informacji o spełnieniu wymagania.
1	Zbieżność oświadczeń osób audytowanych.
2	Informacja udokumentowana.

Lp.	Opis wymagania	Podstawa	Audytowany	Dowody	Ustalenia	Ocena
1	Wyznaczenie osoby do kontaktu	Art. 21 UoKSC	Urząd Gminy w Starym Polu	Kserokopia dokumentu z dnia 9.09.2021r	Wójt wyznaczył Pana Janusza Salomonika jako osobę do kontaktów	2
2	Przekazanie danych osoby wyznaczonej	Art. 22 ust. 1 pkt 5 UoKSC	Urząd Gminy w Starym Polu	Potwierdzenie zgłoszenia osób kontaktowych nr: 1353930	Zgłoszenia dokonano 20.09.2021r.; 3.11.2021 UG otrzymał informacje (mail)o przyjęciu zgłoszenia	2
3	Zapewnienie zarządzania incydentem	Art. 22 ust. 1 pkt 1 UoKSC	Urząd Gminy w Starym Polu	Zarządzenie Nr 59/2021 z 11.08.2021r. wdrażajace PBI	Opisane w:PBI (paragraf 40)	2
4	Zgłaszanie incydentu	Art. 22 ust. 1 pkt 2 UoKSC Art. 23 UoKSC	Urząd Gminy w Starym Polu	Zarządzenie Nr 59/2021 z 11.08.2021r. wdrażajace PBI	Opisane w:PBI (paragraf 40)	2
5	Zapewnienie obsługi incydentu	Art. 22 ust. 1 pkt 3 UoKSC	Urząd Gminy w Starym Polu	Zarządzenie Nr 59/2021 z 11.08.2021r. wdrażajace PBI	Opisane w: PBI (paragraf 40)	2
6	Zapewnienie dostępu do wiedzy	Art. 22 ust. 1 pkt 4 UoKSC	Urząd Gminy w Starym Polu	Brak publikacji	UG nie realizuje wymagań Art.. 22 pkt 4) KSC	0
7	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI	Urząd Gminy w Starym Polu	Brak SZBI	UG nie opracował i nie wdrożył SZBI. UG posiada dokument PBI zawierajacy cząstkowe zapisy wymagane SZBI	0
8	Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI	Urząd Gminy w Starym Polu	Brak SZBI	Brak dokumentu	0
9	Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI	Urząd Gminy w Starym Polu	Brak SZBI	Brak dokumentu	0
10	Aktualizowanie regulacji wewnętrznych	Par. 20 ust. 2 pkt 1 KRI	Urząd Gminy w Starym Polu	Brak SZBI	PBI zawiera zapis dotyczący aktualizacji regulacji wewnętrznych w zakresie zmieniajacego się otoczenia	0
11	Inwentaryzacja sprzętu i oprogramowania	Par. 20 ust. 2 pkt 2 KRI	Urząd Gminy w Starym Polu	Brak pełnej inwentaryzacji sprzetu i oprogramowania	Informatyk stosuje oprogramowanie NMAP do inwenaryzacji sprzetu działającego w sieci	0
12	Przeprowadzanie okresowych analiz ryzyka	Par. 20 ust. 2 pkt 3 KRI	Urząd Gminy w Starym Polu	Brak okresowych analiz ryzyka	Brak dokumentów potwierdzających przeprowadzanie analiz ryzka	0
13	Postępowanie z ryzykiem	Par. 20 ust. 2 pkt 3 KRI	Urząd Gminy w Starym Polu	Nie wystąpiło zdarzenie wymagajace zastosowania postępowania z ryzykiem - brak dokumentów	Rozdział 6 PBI opisuje postępowanie z ryzykiem. Brak działań.	2

Sosnowski

14	Zarządzanie uprawnieniami	Par. 20 ust. 2 pkt 4, 5 KRI	Urząd Gminy w Starym Polu	Brak stosowania opisanego rozwiązania	Rozdział 2 IZSI opisuje postępowanie związane z zarządzaniem uprawnieniami	2
15	Szkolenia i uświadamianie	Par. 20 ust. 2 pkt 6 KRI	Urząd Gminy w Starym Polu	Protokół ze szkolenia IOD z 10-09-2021r.	IOD przeprowadził szkolenie i opracował konspekt szkolenia	2
16	Monitorowanie dostępu do informacji	Par. 20 ust. 2 pkt 7 lit. a KRI	Urząd Gminy w Starym Polu	Brak dokumentów potwierdzających opisane działania	Brak regulacji opisujących sposób monitorowania dostępu do informacji	0
17	Monitorowanie nieautoryzowanych zmian	Par. 20 ust. 2 pkt 7 lit. b KRI	Urząd Gminy w Starym Polu	Brak monitorowania nieutoryzowanych zmian	Brak regulacji opisujących sposób monitorowania nieautoryzowanych zmian	0
18	Zabezpieczenie nieautoryzowanego dostępu	Par. 20 ust. 2 pkt 7 lit. c KRI	Urząd Gminy w Starym Polu	Obserwacja: UG stosuje indywidualne loginy i hasła	PBI (paragraf 34)	2
19	Ustanowienie zasad bezpiecznej pracy mobilnej	Par. 20 ust. 2 pkt 8 KRI	Urząd Gminy w Starym Polu	Brak regulacji	Brak sformalizowanych regulacji	0
20	Zabezpieczenie informacji przed nieuprawnionym ujawnieniem	Par. 20 ust. 2 pkt 9 KRI	Urząd Gminy w Starym Polu	Brak regulacji	UG stosuje indywidualne loginy i hasła oraz gradację uprawnień	1
21	Zabezpieczenie informacji przed nieuprawnioną modyfikacją	Par. 20 ust. 2 pkt 9 KRI	Urząd Gminy w Starym Polu	Brak regulacji	UG stosuje indywidualne loginy i hasła oraz gradację uprawnień	1
22	Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem	Par. 20 ust. 2 pkt 9 KRI	Urząd Gminy w Starym Polu	Brak regulacji	UG stosuje indywidualne loginy i hasła oraz gradację uprawnień	1
23	Zawieranie w umowach serwisowych zapisów o bezpieczeństwie	Par. 20 ust. 2 pkt 10 KRI	Urząd Gminy w Starym Polu	Brak regulacji	Brak regulacji	0
24	Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania	Par. 20 ust. 2 pkt 11 KRI	Urząd Gminy w Starym Polu	Brak regulacji	Brak regulacji	0
25	Aktualizowanie oprogramowania	Par. 20 ust. 2 pkt 12 lit. a KRI	Urząd Gminy w Starym Polu	Obserwacja: ASI na bieąco aktualizuje oprogramowanie, ASI przedstawił log zdarzeń z systemów firmy Radix	Opisane w: IZSI (paragraf 5,18)	2
26	Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu	Par. 20 ust. 2 pkt 12 lit. b KRI	Urząd Gminy w Starym Polu	ASI cyklicznie wykonuje wymagane kopie, brak rejestru - ASI wskazał lokalizacje przechowywanych kopii.	Opisane w: IZSI (paragraf 17)	1
27	Ochrona systemu przed błędami	Par. 20 ust. 2 pkt 12 lit. c KRI	Urząd Gminy w Starym Polu	Brak regulacji	Brak regulacji	0
28	Stosowanie mechanizmów kryptograficznych w systemach	Par. 20 ust. 2 pkt 12 lit. d KRI	Urząd Gminy w Starym Polu	Brak stosowania mechanizmów szyfrujących	Opisane w: IZSI (paragraf 5)	0
29	Zapewnienie bezpieczeństwa plików systemowych	Par. 20 ust. 2 pkt 12 lit. e KRI	Urząd Gminy w Starym Polu	Obserwacja:ASI w sposób cykliczny wykonuje wymagane kopie, odebrane uprawnienia administracyjne	Opisane w: IZSI (paragraf 17)	2
30	Zarządzanie podatnościami systemów	Par. 20 ust. 2 pkt 12 lit. f, g KRI	Urząd Gminy w Starym Polu	Brak zarządzania podatnościami	Brak zapisów regulujących zarządzanie podatnościami	0
31	Kontrola zgodności systemów z regulacjami	Par. 20 ust. 2 pkt 12 lit. h KRI	Urząd Gminy w Starym Polu	Brak dokumentów potwierdzających przeprowadzenie sprawdzenia	Opisane w:PBI (paragraf 30)	0

32	Zapewnienie audytu bezpieczeństwa informacji, nie rzadziej niż raz na rok	Par. 20 ust. 2 pkt 14 KRI	Urząd Gminy w Starym Polu	Brak raportów z audytów	UG nie wykonuje okresowych audytów bezpieczeństwa	0

*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 (Dz.U. z 2017 r. poz. 2247, t.j.)

**Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.).

Centrum Zarządzania Bezpieczeństwem Informacji
Marek Lewandowski
ul. Mała [illegible], 82-400 Sztum
tel. 500 866 061, e-mail: biuro@abi-info.pl
NIP 579-110-31-81

OCENA WYBRANYCH ASPEKTÓW BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Zasady oceny

Każdemu z zagadnień, w polu oznaczonym na żółto, należy przypisać ocenę wg poniższej skali:

0	Całkowity brak realizacji wymagania. Brak świadomości wymogu.
1	Wymaganie spełnione w małym stopniu. Świadomość istnienia wymagania.
2	Częściowa realizacja wymagania.
3	Drobne niedociągnięcia, niewpływające na bezpieczeństwo IT.
4	Pełna zgodność z wymaganiami.

Lp.	Zagadnienie	Ustalenia	Ocena
1	**Dokumentacja potwierdzająca wykonane działania wskazanego w ustawie o krajowym systemie cyberbezpieczeństwa***		3
1.1	Czy zostały zidentyfikowane usługi publiczne, których świadczenie zależy od bezpieczeństwa systemów informacyjnych?	TAK, systemy podatkowe oraz EOD	
1.2	Czy zostały wskazane osoby (podmioty) odpowiedzialne za zarządzanie incydentami?	TAK;Wynika z Polityki Bezpieczeństwa Informacji w UG Stare Pole 11 08 2022r. §7	
1.3	Czy podmiot publiczny realizuje zadania publikowania informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa oraz możliwych, skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, tj. zadań zawartych w art. 22 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?	NIE	

1.4	Czy została wyznaczona i zgłoszona do właściwego CSIRT, osoba kontaktowa, o której mowa w art. 21 oraz art. 22 ust. 1 pkt 5 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?	TAK; Informatyk Janusz Salamonik - 9.09.2021r.	
2	**Opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne**		0
2.1	Czy wszystkie elementy składowe systemu informatycznego zostały zinwentaryzowane?	NIE	
2.2	Czy dla każdego systemu informatycznego utrzymywana jest aktualna lista osób odpowiedzialnych za jego bezpieczną eksploatację?	NIE	
3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**		0
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?	NIE	
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?	NIE	
3.3	Czy istnieje dokumentacja architektury sieci?	NIE	
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?	NIE	
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?	NIE	
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?	NIE	

3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?	NIE	
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?	TAK, w zakresie zakupionego sprzętu komputerowego	
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?	NIE	
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?	NIE	
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?	NIE	
4	**Dokumentacja procesu zarządzania incydentami**		2
4.1	Czy wdrożone jest monitorowanie i wykrywanie incydentów? Kto za nie odpowiada? (stanowiska, funkcje itp. - bez danych osobowych)	Tylko w zakresie incydentów wynikajacych z RODO, odpowiada IOD	
4.2	Czy istnieje procedura informowania o wykrytych incydentach?	TAK	
4.3	Czy istnieją procedury reagowania na incydenty?	Tylko w zakresie incydentów wynikających z RODO	
5	**Aspekty techniczne do weryfikacji**		

5.1	Wyniki audytu serwisów WWW z uwzględnieniem: - wersji serwera HTTP; - wersji systemu CMS (o ile występuje); - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.); - dostępności kompetentnego personelu do utrzymania serwisów.	UG stosuje: apache:tomcat:9.0.40; UG stosuje: TLS 1.2 UG nie posiada własnego CMS; UG nie stosuje Certyfikatów X.509; UG nie stosuje algorytmów kryptograficznych; Personel IT nie zapewnia pełnych komeptencji	0
5.2	Wyniki audytu serwisów pocztowych z uwzględnieniem: - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów.	Nie wdrożono mechanizmu Sender Policy Framework; Nie wdrożono mechanizmu DomainKeys Identified Mail; Nie wdrożono mechanizmu Domain-based Message Authentication; Stosowane jest szyfrowanie TLSv1.2 Personel IT nie zapewnia pełnych kompetencji.	0
5.3	Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem: - wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację; - stosowania mechanizmów segmentacji sieci; - izolacji urządzeń końcowych użytkowników; - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji; - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa; - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.	Wdrżono system Bitdefender z centralną kosolą Brak prawidłowej segmentacji sieci; Brak izolacji urządzeń końcowych; Proces tworzenia kopii został opisany w IZSI - brak wskazania systemów i programów podlegających kopiom, brak wskazania sposóbu i częstotliwości odzyskania danych; Brak monitorowania ruchu wewnątrz sieci; Personel IT nie zapewnia pełnych kompetencji	0
5.4	Wyniki audytu połączenia z siecią Internet z uwzględnieniem: - monitorowania ruchu wchodzącego i wychodzącego; - stosowanych zabezpieczeń przed atakami DDoS; - stosowanych zabezpieczeń przed wyciekiem informacji (DLP); - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.); - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.	Brak monitorowania ruchu wchodzącego i wychodzącego; Brak stosowania mechanizmów przed atakami DDoS; Brak systemu DLP; Brak systemów stosowanych do zabezpieczeń punktu styku; Personel IT nie zapewnia pełnych kompetencji	0

6	**Aspekty organizacyjne do weryfikacji**		
6.1	Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem: - regularnego identyfikowania znanych podatności w eksploatowanych systemach IT; - terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników; - prowadzenia okresowego przeglądu uprawnień użytkowników; - prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń.	Brak regularego idetyfikowania podatności; Dane do systemów zarządzania tożsamością i urawnieniami użytkownikó nie są terminowo wprowadzane ani aktualizowane; Brak okresowych przeglądów uprawnień; ASI okresowo prowadzi nieudokumentowane szkolenia podnoszące świadomość w zakresie zagrożeń.	0
6.2	Wyniki audytu procesów planowania z uwzględnieniem: - posiadania planów przywracania usług IT na wypadek awarii; - prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT; - cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.	Brak planów przywracania usług IT na wypadek awarii; Brak przegolądów oraz doskonalenia planów przywracania usług IT; UG użytkuje systemy nie posiadające wsparcia producenta. Brak reguacji opisujacej cykl życia ststemów IT i eksploatacji produktów nieposiadających	0

*Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.).

Centrum Zarządzania Bezpieczeństwem Informacji
Jacek Lewandowski
ul. Morawskiego 10/11, 82-400 Sztum
tel. 500 966 061, e-mail: biuro@abi-info.pl
NIP 578-110-31-81