



# GMINA MALCZYCE

55-320 Malczyce, ul. Traugutta 15, tel. 71/317 92 23, fax 71/317 96 17

[www.malczyce.wroc.pl](http://www.malczyce.wroc.pl), e-mail: [sekretariat@malczyce.wroc.pl](mailto:sekretariat@malczyce.wroc.pl)

Malczyce, dnia 22 maja 2024 roku

RR.526.3.1.2024.JP

**G1ANT ROBOT Sp. z o.o.**  
**ul. Stepowa 34D**  
**30-698 Kraków**

Dotyczy: petycji nr 2024/1 z dnia 6 maja 2024.

Zgodnie z art. 2 oraz art. 13 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r., poz. 902) Wójt Gminy Malczyce udziela następującej odpowiedzi:

W związku z otrzymaną prośbą o udostępnienie informacji publicznej z dnia 08.05.2024 (wpływ mailem na adres: [j.ptaszynska@malczyce.wroc.pl](mailto:j.ptaszynska@malczyce.wroc.pl)) o następującej treści:

## 1. Wniosek o informacje dotyczące inicjatywy dotacji 50 000 zł

Wnosimy o udzielenie informacji publicznej o konkretną informację na temat planów i terminów, które Urząd zamierza zastosować w zakresie pozyskania nieodpłatnej dotacji na cyfryzację w kwocie 50 000 zł oraz intencji rozpoczęcia rozmów na ten temat z wnioskodawcą.

Odpowiedź: Informuję, że Gmina Malczyce planuje pozyskać dotację na cyfryzację urzędu. W związku z powyższym złożyliśmy wniosek o przyznanie dotacji w ramach programu „Cyberbezpieczny Samorząd”. Jesteśmy otwarci na rozmowy w temacie nieodpłatnej dotacji na cyfryzację w kwocie 50 000 zł.

### 1.1 Dane kontaktowe urzędnika

W przypadku twierdzącej odpowiedzi na wniosek z §1, uprzejmie prosimy o przekazanie danych kontaktowych osoby odpowiedzialnej za procesy decyzyjne dotyczące pozyskiwania nieodpłatnych dotacji dla Urzędu. Prosimy również o informacje dotyczące osoby zarządzającej infrastrukturą informatyczną. Dokładne dane powinny obejmować imię i nazwisko, adres e-mail, numer telefonu oraz stanowisko służbowe każdej z wymienionych osób. Dodatkowo, prosimy o informację, kiedy można oczekiwać rozpoczęcia rozmów z Urzędem w sprawie wspomnianej dotacji. Dziękujemy za współpracę i czekamy na szybką odpowiedź w celu dalszego postępowania.

Odpowiedź: Informuję, że osobami odpowiedzialnymi za pozyskiwanie środków zewnętrznych w urzędzie zajmują się:

Joanna Ptaszyńska – Kierownik Referatu Rozwoju, tel. 71/3179223 wew. 220, e-mail: j.ptaszynska@malczyce.wroc.pl

Artur Dychowicz – Insp. ds. pozyskiwania środków z funduszy zewnętrznych, tel. 71/3179223 wew. 220, e-mail: a.dychowicz@malczyce.wroc.pl

Infrastrukturą informatyczną zarządza firma zewnętrzna:

EURONET FHU Dariusz Kubacki, tel: 605 339 669, e-mail: biuro@euronet.wroclaw.pl

Jesteśmy otwarci na rozmowy w temacie nieodpłatnej dotacji na cyfryzację w kwocie 50.000 zł.

## 2. Wniosek o informacje dotyczące audytu i automatyzacji

Wnosimy o udzielenie informacji publicznej na temat przeprowadzenia przez Kierownika JST, w ciągu ostatnich trzech lat, audytu, analizy lub planowania działań systematycznych mających na celu stopniową automatyzację systemów teleinformatycznych używanych w Urzędzie.

Odpowiedź: Informuję, że w ciągu ostatnich trzech latach był przeprowadzony audyt wewnętrzny dot. spełnienia wymagań określonych w KRI.

### 2.1 Szczegóły realizacji działań automatyzacyjnych

W przypadku twierdzącej odpowiedzi na wniosek z §2, prosimy o dostarczenie szczegółowego raportu z przeprowadzonych w ciągu ostatnich trzech lat audytów technologicznych pod kątem automatyzacji Urzędu, w tym ich wyników, wniosków oraz planów wdrożenia rekomendacji.

Należą do nich informacje, w ramach których systemów rozpoczęto automatyzację, jaki zakres działań osiągnięto, czy te działania były wsparte analizą technologiczną, oraz z jakich narzędzi RPA skorzystano. Prosimy również o informacje dotyczące osiągniętych celów związanych z automatyzacją, w tym które oprogramowanie i systemy udało się zintegrować, oraz inne istotne informacje oceniające stopień informatyzacji i automatyzacji Urzędu.

Odpowiedź: Informuję, iż wszelkich odpowiedzi udzielam w dołączonych dokumentach. W załączeniu przesyłam raport, kwestionariusz samooceny, listę czynności, które zostały wykonane w ramach automatyzacji oraz potrzeby wdrożenia systemowego.

Z poważaniem  
**Wójt Gminy Malczyce**  
*Piotr Frankowski*

**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	Zbiżczość oświadczeń osób audytowanych.
2	Informacja udokumentowana.

Lp.	Opis wymagania	Podstawa	Audytowany	Dowody	Ustalenia	Ocena
1	Wyznaczenie osoby do kontaktu	Art. 21 UoKSC	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska	Zarządzeniem nr 005022R2022 Wójta Gminy Malczyce z dnia 1 marca 2022 r. powołana została osoba odpowiedzialna za zarządzanie incydentami w Gminie.		2
2	Przekazanie danych osoby wyznaczonej	Art. 22 ust. 1 pkt 5 UoKSC	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Pracownik został zgłoszony do NASK pod numerem 1564631 w dniu 03.03.2022 r.		2
3	Zapewnienie zarządzania incydem	Art. 22 ust. 1 pkt 1 UoKSC	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak zasad.	Wymagania UoKSC nie zostały ujęte w obowiązującej dokumentacji.	0
4	Zgłaszanie incydentu	Art. 22 ust. 1 pkt 2 UoKSC Art. 23 UoKSC	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak zasad zarządzania incydentami, rejestr nie zawiera żadnych zapisów.	Wymagania UoKSC nie zostały ujęte w obowiązującej dokumentacji.	0
5	Zapewnienie obsługi incydentu	Art. 22 ust. 1 pkt 3 UoKSC	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Wyznaczona została osoba do obsługi incydentów (Zarządzeniem nr 005022R2022 Wójta Gminy Malczyce z dnia 1 marca 2022 r.)	Pracownicy urzędu obsługują incydenty na podstawie dokumentacji dotyczącej RODO.	1
6	Zapewnienie dostępu do wiedzy	Art. 22 ust. 1 pkt 4 UoKSC	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	odpowiednie informacje znajdują się na stronie: <a href="https://bip.malczyce.wroc.pl/index.php/cyberbezpiectwo">https://bip.malczyce.wroc.pl/index.php/cyberbezpiectwo</a>		2
7	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	W Urzędzie obowiązuje Polityka bezpieczeństwa oraz instrukcja zarządzania. Pełen system SZBI nie został wprowadzony.	0
8	Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	j.w.	0
9	Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	j.w.	0
10	Aktualizowanie regulacji wewnętrznych	Par. 20 ust. 2 pkt 1 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	Instrukcja zarządzania systemami informatycznymi została wprowadzona 31.08.2018 r. Do dnia diagnozy nie zostały wprowadzone zmiany w dokumentacji.	0
11	Inwentaryzacja sprzętu i oprogramowania	Par. 20 ust. 2 pkt 2 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Cyklicznie wykonywany jest spis z natury, które obejmuje zakupiony sprzęt elektroniczny oraz oprogramowanie. Arkusz spisu z natury Nr 9 - serwerownia. Księga inwentarzowa K-10.020.	Spis nie obejmuje wszystkich komponentów infrastruktury teleinformatycznej.	1
12	Przeprowadzanie okresowych analiz ryzyka	Par. 20 ust. 2 pkt 3 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Wskazano zasady zarządzania ryzykiem oraz wyniki przeprowadzonej analizy.	Ocena analizy ryzyka nie uwzględnia aktualnego stanu zabezpieczeń systemów informatycznych.	1
13	Postępowanie z ryzykiem	Par. 20 ust. 2 pkt 3 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Kolumna zalecenia w analizie ryzyka.	Nie wszystkie zabezpieczenia zostały wprowadzone.	1

14	Zarządzanie uprawnieniami	Par. 20 ust. 2 pkt 4, 5 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Zasady zarządzania uprawnieniami znajdują się w Instrukcji zarządzania systemem informatycznym w Urzędzie Gminy Malczyce par. 8 - 9 - 10.	Urząd nie stosuje zasad zarządzania uprawnieniami, brak wniosków o nadanie i odebranie uprawnień, brak rejestrów. Stwierdzono nieaktualne uprawnienia w systemach.	0
15	Szkolenia i uświadamianie	Par. 20 ust. 2 pkt 6 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak dowodów na przeprowadzenie szkoleń z zakresu bezpieczeństwa teleinformatycznego.	Brak dowodów na przeprowadzenie szkoleń z zakresu bezpieczeństwa teleinformatycznego.	0
16	Monitorowanie dostępu do informacji	Par. 20 ust. 2 pkt 7 lit. a KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Na styku z siecią nie jest monitorowany dostęp do informacji. Brak monitorowania wiadomości pocztowych. SVGID - brak możliwości identyfikacji czynności wykonywanych przez pracowników.	Systemy informatyczne nie są objęte monitorowaniem.	0
17	Monitorowanie nieautoryzowanych zmian	Par. 20 ust. 2 pkt 7 lit. b KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	Dostęp do plików znajdujących się na dysku sieciowym jest niemożliwy, z powodu wykorzystania jednego identyfikatora przez wszystkich pracowników.	0
18	Zabezpieczenie nieautoryzowanego dostępu	Par. 20 ust. 2 pkt 7 lit. c KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	W systemach informatycznych stosowane są indywidualne konta nadawane pracownikom. Kontrolą objęto systemy sygid, Bestia i BIP.	Poza dyskami sieciowymi nie stwierdzono systemów z nieautoryzowanym dostępem.	1
19	Ustanowienie zasad bezpiecznej pracy mobilnej	Par. 20 ust. 2 pkt 8 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Zasady bezpiecznej pracy zostały określone w zarządzeniu nr 81 z 2020 roku Par. 8 Postępowanie ze sprzętem informatycznym, w tym nośnikami danych wykorzystywanym w pracy zdalnej.		2
20	Zabezpieczenie informacji przed nieuprawnionym ujawnieniem	Par. 20 ust. 2 pkt 9 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	W Instrukcji zarządzania systemami informatycznymi wprowadzono zasady zarządzania hasłami, uprawnieniami, zasady zarządzania kluczami kryptograficznymi, zasady zabezpieczenia sieci, procedury rozpoczęcia, zawieszenia i zakończenia pracy.		2
21	Zabezpieczenie informacji przed nieuprawnioną modyfikacją	Par. 20 ust. 2 pkt 9 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak zabezpieczeń danych znajdujących się na dyskach wspólnych.	Aktualna konfiguracja pozwala pracownikom na usuwanie plików na dyskach sieciowych wraz z kopiami zapasowymi.	0
22	Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem	Par. 20 ust. 2 pkt 9 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Informacje przed zniszczeniem chronione są za pomocą kopii zapasowych. W instrukcji wprowadzono zasady tworzenia kopii zapasowych, kopie wykonywane są w cyklu dziennym oraz tygodniowym.		2
23	Zawieranie w umowach serwisowych zapisów o bezpieczeństwie	Par. 20 ust. 2 pkt 10 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	Umowy obejmują wymagania RODO, nie uwzględniają wymagań KRI.	0
24	Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania	Par. 20 ust. 2 pkt 11 KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	IZSI zawiera: Zasady rozpoczęcia, zakończenia i zawieszenia pracy, zasady szyfrowania, zasady korzystania z Internetu, zasady postępowania z nośnikami.	Zasady nie są stosowane. Stwierdzono stację roboczą bez oprogramowania antywirusowego, komputer przenośny oraz nośniki wymienne bez mechanizmów szyfrowania.	0
25	Aktualizowanie oprogramowania	Par. 20 ust. 2 pkt 12 lit. a KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Weryfikacją objęto serwer Sygid, CMS Joomla oraz WordPress. Wykorzystywane oprogramowanie jest nieaktualne i zawiera krytyczne podatności bezpieczeństwa.	Najstarsze oprogramowanie nie było aktualizowane przez 10 lat.	0
26	Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu	Par. 20 ust. 2 pkt 12 lit. b KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	IZSI pkt 7 Procedura tworzenia kopii zapasowych.	Wykonywane kopie realizowane są w cyklu dziennym. Kopie zapasowe nie są objęte testowaniem. Brak kopii offline.	1
27	Ochrona systemu przed błędami	Par. 20 ust. 2 pkt 12 lit. c KRI	Anna Rutowicz	System Sygid nie kontroluje danych wprowadzanych do systemu. Kontrolą objęto pola wprowadzania danych osobowych do systemu.	Aktualnie jedynym zabezpieczeniem przed błędami są kopie zapasowe.	1
28	Stosowanie mechanizmów kryptograficznych w systemach	Par. 20 ust. 2 pkt 12 lit. d KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Komputery przenośne oraz nośniki wymienne nie są szyfrowane. Dostęp do strony internetowej, BIPu oraz poczty posiada poprawne protokoły zabezpieczające połączenie. Kopie zapasowe są szyfrowane za pomocą AFS 256.		1
29	Zapewnienie bezpieczeństwa plików systemowych	Par. 20 ust. 2 pkt 12 lit. e KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	Użytkownicy stacji roboczych działają na kontaktach administracyjnych.	0
30	Zarządzanie podatnościami systemów	Par. 20 ust. 2 pkt 12 lit. f, g KRI	Joanna Piaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	Brak kontroli podatności w użytkowanych systemach.	0

31	Kontrola zgodności systemów z regulacjami	Par. 20 ust. 2 pkt 12 lit. h KRI	Joanna Ptaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	RODO - kontrolą objęto rejestr kategorii czynności przetwarzania. Rejestr nie zawierał czynności związanych z obsługą kadrową danych osobowych.		1
32	Zapewnienie audytu bezpieczeństwa informacji, nie rzadziej niż raz na rok	Par. 20 ust. 2 pkt 14 KRI	Joanna Ptaszyńska, Włodarski Mateusz, Beata Łuckiewicz-Kropska.	Brak.	Urząd nie przeprowadził audytu bezpieczeństwa wymaganego KRI.	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.).

Wykonane czynności w ramach automatyzacji:

1. Wdrożenie ochrony sieci przez sprzętowy firewall Ubiquiti UDM na styku sieci LAN oraz UTM Mikrotik z aktualnymi oprogramowaniami : firewall, VPN, antywirus, IPS
2. Urządzenia mobilne (laptop) Posiadają zabezpieczenia BitLocker oraz zabezpieczone hasłem
3. Wdrożenie Serwera NAS do wykonywania kopii bezpieczeństwa, szyfrowanie AES 256bit dodatkowy antywirus wdrożony na serwerze NAS skanujący kopie bezpieczeństwa
4. Modernizacja Infrastruktury sieci LAN (zminimalizowanie możliwości niekontrolowanego podłączenia do sieci LAN)
5. Automatyczna aktualizacja Sprzętów IT, komputerów PC oraz antywirusów
6. Wymienione upsy w serwerowni oraz skrzyni krosowniczej gops

Potrzebne wdrożenia systemowe:

1. Wdrożenie usługi Domenowej Active Directory dla kontroli logowania użytkowników oraz plików (bezpieczeństwo ruchu w sieci LAN)
2. implementacja protokołu sieciowego warstwy aplikacji LDAP na serwerze dla AD
3. Wymiana serwera SIGID (oprogramowanie serwerowe jest przestarzałe)
4. Wdrożenie dodatkowej Kopii bezpieczeństwa w drugim miejscu budynku
5. Modernizacja strony internetowej na nową wersję
6. Modernizacja strony BIP
7. Zakup Pamięci Pendrive szyfrowanych, oraz określenie identyfikatorów Pamięci zezwolonych urządzeń USB

Spis oprogramowania w Urzędzie Gminy:

1. Obszar finansów i księgowości
  1. SIGID - Zakład Systemów Informatycznych SIGID Sp. z o. o.
  2. SJO BeSTi@ - budżetjst
  3. BeSTi@ - budżetjst
2. Obszar windykacji i opłat
  - 1 SIGID - Zakład Systemów Informatycznych SIGID Sp. z o. o.
3. Obszar kadr i płac
  1. Płatnik - ZUS
  2. SIGID - Zakład Systemów Informatycznych SIGID Sp. z o. o.
4. Obszar e-Usług dla mieszkańców
  1. posiedzenia.pl - GK Pro sp. z o.o. sp.k.
  2. Moje odpady - Waste24 Sp. z o.o.
5. Obszar elektronicznego obiegu dokumentów  
W trakcie wdrażania

1. EZD RP - Naukowa i Akademicka Sieć Komputerowa – Państwowy  
Instytut Badawczy w partnerstwie z Wojewodą Podlaskim

6. Obszar konsultacji społecznych

1. Facebook

Osoba odpowiedzialna: Dariusz Kubacki, EURONET FHU

L.p.	Obszar/wymagania	Samoocena spełnienia wymagań S/N/CS <sup>1</sup> w 2022 r.	Samoocena spełnienia wymagań S/N/CS w 2023 r.	Stawisko/Osoba udzielająca odpowiedzi <sup>2</sup>	Podstawa prawna	Dokumenty <sup>3</sup> /informacje potwierdzające spełnienie wymagań <sup>4</sup> i świadczące o rozwoju systemu bezpieczeństwa informacji (wypełniono w 2022 r.)	Dokumenty/informacje potwierdzające spełnienie wymagań i świadczące o rozwoju systemu bezpieczeństwa informacji (wypełniono w 2023 r.)
1.	2.	3.	4.	5.	6.	7.	8.
1	Wdrożenie SZBI						
1.1	Czy wdrożono system zarządzania bezpieczeństwem informacji (SZBI) zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, niezawodność, niezawodność i niezawodność?	CS	CS	IOD	§ 20 ust. 1 Rozporządzenia KRI	W urzędzie obowiązuje Polityka bezpieczeństwa oraz instrukcja zarządzania bezpieczeństwem. Pełen system SZBI nie został jeszcze wprowadzony.	
2	Aktualizacja regulacji wewnętrznych						
2.1	Czy zapewniono aktualizacje regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia?	N	CS	IOD	§ 20 ust. 2 pkt 1 Rozporządzenia KRI	Aktualizacja wewnętrznych regulacji w trakcie przygotowania.	
3	Aktualność inwentaryzacji sprzętu i oprogramowania						
3.1	Czy utrzymywana jest aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację?	N	CS	ASI	§ 20 ust. 2 pkt 2 Rozporządzenia	Prowadzona jest dokumentacja papierowa każdej stacji PC (np. faktury, licencje).	

<b>4. Okresowa analiza ryzyka bezpieczeństwa informacji</b>					
	CS	CS	ASI	§ 20 ust. 2 pkt 3 Rozporządzenia KRI	Do okresowej analizy ryzyka zostanie uwzględniony aktualny stan zabezpieczeń systemów informatycznych.
4.1	Czy przeprowadzana jest okresowa analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowane są działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy?	CS			
<b>5 Adekwatne uprawnienia i zmiana uprawnień</b>					
5.1	Czy podejmowane są działania zapewniające, 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?	CS	S	ASI	Upoważnienia wypełnia zgodnie z dokumentacją. gmina
5.2	Czy bezzwłocznie zmieniane są uprawnienia, w przypadku zmiany zadań zaangażowanych w proces przetwarzania informacji?	S	S	ASI	Uprawnienia są wydawane/ zmieniane/wyrejestrowywane na wniosek Pani Sekretarz.

<b>6</b>	<b>Szkolenia dot. bezpieczeństwa informacji</b>	CS	IOD	§ 20 ust. 2 pkt 6 Rozporządzenia KRI	Nie wystąpiły istotne incydenty. W przypadku wystąpienia incydentu, będą wykonywane dodatkowe szkolenia.		
6.1	Czy zapewniono szkolenia osobom zaangażowanym w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: - zagrożenia bezpieczeństwa informacji; - skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, - stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia oprogramowanie minimalizujące ryzyko błędów ludzkich?						
<b>7.</b>	<b>Ochrona informacji</b>	N	CS	ASI	§ 20 ust. 2 pkt 7 Rozporządzenia KRI	Gmina nie posiada usługi Active Directory planowane wdrożenie na rok 2023 Dodatkowo wprowadzono blokadę ekranu wygaszaczem ekranu i koniecznością odblokowania hasłem. Monitorowanie i blokowanie dostępu do nośników wymiennych - brak Ochrona sieci LAN na styku z Internetem realizowana jest przez nowy UTM f-my Mikrotik, z aktualnymi oprogramowaniem : firewall, VPN, antywirus, IPS	
7.1	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: - monitorowanie dostępu do informacji, - zmierzające do wykrycia nieautoryzowanych						

	działań związanych z przetwarzaniem informacji, - zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji?	S	S	ASI			(ochrona przed atakami), filtrowanie treści WWW, ochrona przed spamem poprzez program F-Security  Urząd Gminy zabezpieczone systemem antywirusowym. Prowadzony monitoring wizyjny budynku. Stacje robocze zabezpieczone systemem antywirusowym.	
7.2	Czy ustanowiono podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość?	S	S	ASI		§ 20 ust. 2 pkt 8 Rozporządzenia KRI	Nie występuje praca mobilna. Posiadamy jeden laptop Wójta z włączoną funkcją BitLockera. Planowane wdrożenie rok 2023.	
7.3	Czy zabezpieczono informacje w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie?	N	S	ASI		§ 20 ust. 2 pkt 9 Rozporządzenia KRI	Opisy w pkt. 7.1 i 8.1	
7.4	Czy zawierane są w umowach serwisowych podpisanych ze stronami trzecimi zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji?			IOD		§ 20 ust. 2 pkt 10 Rozporządzenia KRI	Z podmiotami są zawarte umowy powierzenia.	
7.5	Czy ustalono zasady postępowania z informacjami, zapewnijające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych?			IOD		§ 20 ust. 2 pkt 11 Rozporządzenia KRI	Urządzenia mobilne wynoszone poza obiekt Urzędu zabezpieczone są hasłem.	

8.	Bezpieczeństwo systemów, logi	N	S	ASI	§ 20 ust. 2 pkt 12 Rozporządzenia KRI	
8.1	<p>Czy zapewniono odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:</p> <ul style="list-style-type: none"> <li>- dbałości o aktualizację oprogramowania,</li> <li>- minimalizowaniu ryzyka utraty informacji w wyniku awarii,</li> <li>- ochronie przed błędami, przed nieuprawnioną modyfikacją,</li> <li>- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa,</li> <li>- zapewnieniu bezpieczeństwa plików systemowych,</li> <li>- redukcji ryzyk z wynikających wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,</li> <li>- niezwłocznym podejmowaniu działań po dostrzeżeniu nieuwzględnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,</li> <li>- kontroli zgodności systemów teleinformatycznych</li> </ul>				<p>Utrzymanie poprawnej konfiguracji stacji PC umożliwiającej automatyczne pobieranie aktualizacji systemu operacyjnego. Dodatkowo stan aktualności systemu operacyjnego i oprogramowania antywirusowego realizowany jest automatycznie.</p> <p>Ochrona danych serwerów i kluczowych stacji PC Urzędu realizowana jest przez kompleksowy system backupu. Na system ten składa się dedykowane oprogramowanie Cobian Backup</p> <p>- Urządzenie brzegowe UTM,</p> <p>- wykonywanie kopii zapasowych przez służące do tego celu oprogramowanie,</p> <p>- wykonywanie kopii zapasowej baz danych na nośnik fizycznie wyłączony z sieci,</p>	

	z odpowiednimi normami i politykami bezpieczeństwa?							
8.2	Czy bezzwłocznie zgłaszano incydenty naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących?			IOD		§ 20 ust. 2 pkt 13 Rozporządzenia KRI	Nie wystąpił incydent naruszenia bezpieczeństwa informacji.	
<b>9</b>	<b>Okresowy audyt wewnętrzny</b>							
9.1	Czy zapewniono okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok?			IOD		§ 20 ust. 2 pkt 14 Rozporządzenia KRI	tak	

1 Proszę dokonać samooceny spełnienia wymagania:

S- wymaganie spełnione,  
N – wymaganie niespełnione,  
CS – wymaganie częściowo spełnione.

2 Proszę wskazać osobę udzielającą odpowiedź, posiadającą wiedzę źródłową w zakresie danego wymagania.

3 Proszę podać nazwy i sygnatury dokumentów potwierdzających spełnienie wymagania np. Polityka Bezpieczeństwa Informacji (BI) oraz inne dokumenty stanowiące SZBI, Regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych, Regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w urzędzie. Dokumentacja zarządzania ryzykiem w tym: procedura przeprowadzania analizy ryzyka, rejestr ryzyk, plan postępowania z ryzykiem, dowody utrzymywania i doskonalenia systemu zarządzania ryzykiem oraz dokumentacja zmian w zabezpieczeniach związanych z bieżącą analizą ryzyka. Regulacje wewnętrzne opisujące zarządzanie uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych, Dokumentacja z przeprowadzonych szkoleń pracowników zaangażowanych w proces przetwarzania informacji pod kątem zakresu tematycznego, Regulacje wewnętrzne zawierające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, Regulacje wewnętrzne, w których określono zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych, w tym wymagane klauzule prawne dotyczące BI, umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI.

4 Proszę podać dodatkowe informacje np. odnośnie stosowanych zabezpieczeń systemowych, opis programów itp., natomiast w przypadku niespełnienia wymagań proszę podać przyczynę, również w przypadku częściowego spełnienia wymagań proszę o podanie przyczyn jedynie częściowego spełnienia wymagań.