Wojewoda Zachodniopomorski

K-2.431.1.45.2024.9.IO

Szczecin, 28 marca 2025 r.

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	Działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.
Nazwa i adres organu kontrolującego	Wojewoda Zachodniopomorski, ul. Wały Chrobrego 4, 70-502 Szczecin.
Nazwa i adres organu kontrolowanego	Wójt Gminy Świeszyno, Świeszyno 71, 76-024 Świeszyno.
Osoba pełniąca funkcję Wójta Gminy Świeszyno w okresie objętym kontrolą	Pan Marek Brzostko
Okres objęty kontrolą	od dnia 1 stycznia 2021 r. do dnia 18 listopada 2024 r.
Kontrolerzy	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, kierownik zespołu kontrolnego, Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 77/24 z dnia 12 listopada 2024 r.
Podstawy prawne do przeprowadzenia kontroli	– art. 6 ust. 4 pkt 3 w związku z art. 2 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1]; – art. 25 ust. 1 pkt 3 lit. a, w związku z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2].
Kryteria prowadzenia kontroli	legalność, rzetelność
Rodzaj kontroli i tryb kontroli	kontrola planowa, tryb zwykły
Termin kontroli	11 - 18 listopada 2024 r.
Osoby udzielające wyjaśnień w trakcie kontroli	(XXX) zastępca Wójta, (XXX) Sekretarz, Pan (XXX) zajmujący się obsługą informatyczną Urzędu Gminy Świeszyno, na mocy *Umowy na świadczenie usług informatycznych*[3].

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.
[3] Zwany dalej Informatykiem.

Obszar kontroli Nr 1: Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1.1 Współpraca systemów teleinformatycznych z innymi systemami.
Podstawa prawna: § 5 ust. 3 pkt 3 rozporządzenia KRI[4]: *Interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;* **§ 16 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*
Ustalenia kontroli
Na podstawie przedstawionej dokumentacji ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Świeszyno wykorzystywano system centralny (aplikacja Źródło i Karta Dużej Rodziny) oraz system informatyczny wspomagający obsługę spraw obywatelskich (XXX). System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami Urzędu, jak i innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. System centralny podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu oraz zabezpieczeń związanych z dostępem do systemu.

(dowód: akta kontroli str. 52-53)

1.2 Formaty danych udostępniane przez systemy teleinformatyczne.
Podstawa prawna: § 17 ust. 1 rozporządzenia KRI: *Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;* **§ 18 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;* **§ 18 ust. 2 rozporządzenia KRI:** *Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.*
Ustalenia kontroli
System informatyczny wykorzystywany do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Świeszyno wymieniał dane w formatach określonych w § 18 ust. 1 rozporządzenia KRI o udostępnianiu zasobów

[4] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 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. 2024 poz. 773), zwane dalej „rozporządzeniem KRI".

informacyjnych w co najmniej w jednym z formatów wymienionych w załączniku nr 2 do rozporządzenia.

Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1	Nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.
Ocena obszaru kontroli	**Pozytywna**

Obszar kontroli Nr 2: System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

2.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu.

Podstawa prawna: § 19 ust. 1 rozporządzenia KRI: *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża 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;* **§ 19 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*

Ustalenia kontroli

Wymagania dotyczące systemów teleinformatycznych, w których przetwarzane są rejestry publiczne w postaci teleinformatycznej określone zostały w § 19 ust. 1 rozporządzenia KRI. Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.

W Urzędzie Gminy Świeszyno, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie Nr 279/VIII/2020 Wójta Gminy Świeszyno z dnia 7 lipca 2020r. w sprawie Polityki bezpieczeństwa informacji, w tym danych osobowych;*
- *Zarządzenie Nr 585/VIII/2022 Wójta Gminy Świeszyno z dnia 11 maja 2022r. w sprawie zmiany załącznika Nr 1 do zarządzenia Nr 279/VIII/2020 Wójta Gminy Świeszyno z dnia 7 lipca 2020 r. w sprawie Polityki bezpieczeństwa informacji, w tym danych osobowych.*

W wyniku analizy aktualnej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury spełniają wymogi określone w § 19 ust. 1 i 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. Dokumentacja zawiera między innymi definicję bezpieczeństwa informacji; oświadczenie o intencjach kierownictwa; wyjaśnienie zasad, norm i wymagań mających szczególne znaczenie dla organizacji; określenie sposobu i wskazanie osób realizujących obowiązki wynikające z rozporządzenia KRI.

(dowód: akta kontroli str. 72-163)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji.

Podstawa prawna: § 19 ust. 2 pkt 3 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

Ustalenia kontroli
Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarządzania bezpieczeństwem informacji, pozwalającym na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk.
Procedura szacowania ryzyka powinna być przeprowadzana okresowo, jednak zawsze w przypadku pojawienia się nowych zagrożeń, co wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie.
Kontrolującym przedstawiono następujące materiały dotyczące okresu objętego weryfikacją:

- Metodyka zarządzania ryzykiem w ochronie informacji w tym danych osobowych, Świeszyno 2020,
- Raport z analizy ryzyka w Urzędzie Gminy Świeszyno, Świeszyno 71, 76-024 Świeszyno, data dokumentu 28.08.2024.

Okazane dokumenty wypełniają dyspozycję § 19 ust. 2 pkt 3 rozporządzenia KRI.
(dowód: akta kontroli str. 71, 175-209, 226-261)

2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego.
Podstawa prawna: § 19 ust. 2 pkt 2 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj*
i konfigurację.
Ustalenia kontroli
Inwentaryzacja sprzętu informatycznego powinna zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.
Inwentaryzacja zasobów informatycznych w Urzędzie jest realizowana w wersji elektronicznej przy wykorzystaniu oprogramowania eAuditor. System umożliwia prowadzenie inwentaryzacji generując raporty zawierające informacje dotyczące m. in. sprzętu i oprogramowania oraz rodzaju systemu operacyjnego. W trakcie kontroli okazano stosowną dokumentację, potwierdzającą prowadzenie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych.
Podstawa prawna: § 19 ust. 2 pkt 4 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: 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;*
§ 19 ust. 2 pkt 5 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*
Ustalenia kontroli
Przepisy § 19 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI stanowią m.in, że kierownictwo podmiotu publicznego w celu zapewnienia bezpieczeństwa informacji powinno podjąć działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, adekwatne do realizowanych zadań, a także podjąć bezzwłoczne działania w przypadku zmiany zadań tych osób. Przetwarzanie informacji

w systemach teleinformatycznych wymaga by dostęp do danych realizowany był przez uprawnione osoby, w ściśle ustalonym zakresie.
Kwestie nadawania i odbierania uprawnień do pracy w systemie informatycznym uregulowano w *Polityce bezpieczeństwa informacji w tym danych osobowych*, w rozdziałach:

- VII - *Upoważnienie do przetwarzania danych osobowych*,
- XII – *Nadawanie i zmiany uprawnień do przetwarzania informacji w tym danych osobowych oraz środki uwierzytelnienia*.

Zgodnie z zapisami procedur *do przetwarzania danych osobowych mogą być dopuszczone tylko osoby posiadające pisemne polecenie (w tym upoważnienie do przetwarzania danych osobowych) wydane przez ADO[5]. Dostęp do systemów informatycznych z odpowiednimi uprawnieniami przydzielany jest na podstawie wniosku Kierownika komórki organizacyjnej przesłanego drogą elektroniczną do ASI[6].*
Kontrolującym przedstawiono:

- *Upoważnienie do przetwarzania informacji w tym danych osobowych* wystawione pracownikowi realizującemu zadania zlecone z zakresu administracji rządowej. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności,
- *Oświadczenie,* w którym zawarto miedzy innymi zobowiązanie pracownika do zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania w trakcie zatrudnienia, jak również po ustaniu stosunku pracy.

Z uwagi na fakt, że w okresie podlegającym badaniu, nie wystąpiły przypadki cofania uprawnień nadanych pracownikom realizującym zadania zlecone z zakresu administracji rządowej, nie dokonano sprawdzenia blokowania dostępu do systemów informatycznych.

(dowód: akta kontroli str. 101-103, 111-113, 287-291, 310)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.
Podstawa prawna: § 19 ust. 2 pkt 6 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*
Ustalenia kontroli
11 stycznia 2024 r. w Urzędzie Gminy Świeszyno przeprowadzono szkolenie pracowników z zakresu ochrony danych osobowych. Udział w szkoleniu dokumentowała lista obecności zawierająca imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w szkoleniu wzięli udział pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.
Zgodnie z wyjaśnieniami Wójta z dnia 13 listopada 2024 r. *szkolenia z zakresu ochrony danych osobowych są cyklicznie realizowane raz w roku*, jednak Jednostka nie posiada list obecności z innych lat (poza przedstawioną listą z 2024 r).
Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Istotne jest by szkolenia, których celem jest zagwarantowanie bezpieczeństwa

[5] ADO- Administrator Danych Osobowych.
[6] ASI- Administrator Systemu Informatycznego.

w zakresie przetwarzania informacji, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych miały charakter cykliczny.
Z analizy okazanych dokumentów oraz przedstawionych wyjaśnień wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 262-284)

2.6 Praca na odległość i mobilne przetwarzanie danych.

Podstawa prawna: § 19 ust. 2 pkt 8 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Ustalenia kontroli

Zasady prowadzenia pracy zdalnej zostały uregulowane w rozdziale XX *Polityki bezpieczeństwa informacji, w tym danych osobowych - Praca poza siedzibą Administratora, w tym praca zdalna*. Kwestie bezpiecznego korzystania z urządzeń przenośnych szczegółowo opisano w rozdziale XVII Polityki - *Użytkowanie komputerów przenośnych*.
Procedury przyjęte w Jednostce określają zasady bezpiecznej pracy przy przetwarzaniu mobilnym i w przypadku świadczenia pracy na odległość, zgodnie z § 19 ust. 2 pkt 8 rozporządzenia KRI.
Zgodnie z wyjaśnieniami Wójta z dnia 13 listopada 2024 r. do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie nie wykorzystywano urządzeń mobilnych i nie realizowano pracy na odległość.

(dowód: akta kontroli str. 122-123, 130-132, 310)

2.7 Serwis sprzętu informatycznego i oprogramowania.

Podstawa prawna: § 19 ust. 2 pkt 10 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

Ustalenia kontroli

Obsługa informatyczna Urzędu realizowana jest na podstawie *Umowy na świadczenie usług informatycznych* (XXX).[7] Obsługa informatyczna wg. zapisów umowy obejmuje między innymi następujące czynności: pełnienie funkcji administratora systemu informatycznego, instalację i konfigurację oprogramowania i sprzętu komputerowego, nadzór nad prawidłowym działaniem systemów informatycznych, konserwację i naprawę sprzętu, wykonywanie kopii zapasowych, nadzór nad bezpieczeństwem danych w systemach informatycznych, świadczenie pomocy technicznej związanej z obsługą sprzętu oraz prowadzenie szkoleń w tym zakresie. W umowie uregulowano kwestię czasu reakcji na zgłoszenie konieczności realizacji zadań wynikających z jej zapisów.
W celu realizacji zadań z zakresu administracji rządowej (XXX) zawarto umowę, której przedmiotem jest prowadzeniu nadzoru i serwisu oprogramowania użytkowanego systemu (XXX).[8] Stwierdzono, że w powyższej umowie wprowadzono zapis określający maksymalny czas skutecznej naprawy oprogramowania, czym wypełniono dyspozycję § 19 ust. 2 pkt 10 rozporządzenia KRI, zawierając zapisy gwarantujące odpowiedni

[7] Umowa nr ZW 3/2023 z dnia 20.12.2023 r.

[8] Umowa nr 14854 z dnia 21.12.2022 r.

poziom bezpieczeństwa informacji. W powyższej umowie uregulowano również kwestie powierzenia przetwarzania danych osobowych.

(dowód: akta kontroli str. 292-301)

2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Podstawa prawna: § 19 ust. 2 pkt 13 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Ustalenia kontroli

W *Polityce bezpieczeństwa informacji, w tym danych osobowych;* w rozdziale XVIII *Postępowanie w sytuacji naruszenie bezpieczeństwa informacji w tym danych osobowych* określono sposób postępowania w przypadku stwierdzenia zaistnienia incydentu związanego z bezpieczeństwem informacji oraz wskazując zasady postępowania
w przypadku takiego naruszenia. Przedstawiono jednocześnie katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia. Ponadto instrukcja postępowania w sytuacji wystąpienia incydentów przypisuje odpowiednie zadania IOD[9], ADO oraz ASI w przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji. Kontrolującym przedstawiono *Rejestr incydentów i zagrożeń bezpieczeństwa oraz działań korygujących i zabezpieczających,* w którym odnotowano jedno zdarzenie, zaklasyfikowane jako naruszenie skutkujące koniecznością zgłoszenia tego faktu organowi nadzorczemu.

(dowód: akta kontroli str. 124-127, 285-286)

2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Podstawa prawna: § 19 ust. 2 pkt 14 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

Ustalenia kontroli

W myśl § 19 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- Raport z audytu wewnętrznego informacji w tym danych osobowych przetwarzanych w systemach teleinformatycznych w Urzędzie Gminy Świeszyno, Świeszyno 71, 76-024 Świeszyno za rok 2021;
- Ocena wybranych aspektów bezpieczeństwa systemów informatycznych (2022 r.);
- Raport z analizy ryzyka w Urzędzie Gminy Świeszyno, Świeszyno 71, 76-024 Świeszyno. Dokument dotyczy 2023 r.

W świetle przedstawionych dokumentów oraz złożonych wyjaśnień, należy stwierdzić, że w okresie objętym kontrolą w Jednostce spełniono wymogi określone w § 19 ust. 2 pkt 14 rozporządzenia KRI.

[9] IOD- Inspektor Ochrony Danych.

(dowód: akta kontroli str. 71, 164-225, 310)

2.10 Kopie zapasowe.
Podstawa prawna: § 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych.*
Ustalenia kontroli
Zgodnie z wymogami określonymi w § 19 ust. 2 pkt 12 lit. b) i e) rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.
Zasady wykonywania kopii bezpieczeństwa oraz kwestie ich testowania uregulowano w załączniku nr 16 do *Polityki bezpieczeństwa informacji, w tym danych osobowych; w postaci Procedury tworzenia kopii bezpieczeństwa* oraz w rozdziale XIV wyżej opisanej polityki (*Tworzenie kopii zapasowych i zarządzanie nośnikami elektronicznymi*).
Zgodnie z oświadczeniem Informatyka z dnia 13 listopada 2024 r.:
- kopia stanowiskowa tworzona jest cogodzinnie,
- kopia zapasowa systemów serwerowych wykonywana jest codziennie na dedykowanym urządzeniu do backupu danych,
- raz w miesiącu pełna kopia systemów jest zgrywana na dysk zewnętrzny i przechowywana poza siedzibą Urzędu.

Kopie zapasowe są szyfrowane. W Urzędzie realizowane jest próbne testowane kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania.
(dowód: akta kontroli str. 116-117, 162-163, 302, 304, 312-313)

2.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.
Podstawa prawna: § 15 ust. 1 rozporządzenia KRI: *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje*
z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
Ustalenia kontroli
W celu wykonywania zadań z zakresu administracji rządowej (XXX) zawarto umowę, której przedmiotem jest prowadzeniu nadzoru i serwisu oprogramowania użytkowanych systemów (XXX).
(dowód: akta kontroli str. 296-301)

2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji.
Podstawa prawna: § 19 ust. 2 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:* **pkt 7:** *zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,*
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie

systemów operacyjnych, usług sieciowych i aplikacji; **pkt 9:** *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;* **pkt 11:** *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

Ustalenia kontroli

W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi nadano identyfikator i hasło wejścia do systemów zainstalowanych na komputerach oraz do programów, z których korzystają.

W przypadku systemu „Źródło" dostęp jest możliwy wyłącznie z użyciem karty, na której zapisany jest certyfikat umożliwiający zalogowanie się do centralnego systemu.

Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych.

W wyniku oględzin stanowiska komputerowego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że:

- dostęp do systemu operacyjnego na urządzeniu możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- komputer miał zainstalowane oprogramowanie antywirusowe oraz skonfigurowany wygaszacz ekranu,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitora stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- użytkownikom systemów wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej nie nadano uprawnień administratora, uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń.

(dowód: akta kontroli str. 308-309, 314-315)

2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych.

Podstawa prawna: § 19 ust. 2 pkt 12 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii;*
c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa; **§ 19 ust. 4 rozporządzenia KRI:** *Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

Ustalenia kontroli

- Sieć informatyczną Urzędu zabezpieczono przy wykorzystaniu zapory sieciowej firewall.
- Urząd dysponuje zasilaczem awaryjnym UPS oraz alternatywnym źródłem zasilania -agregatem ATS.
- Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe.
- W Jednostce użytkowany jest router z zapora sieciową, ochroną DDOS.
- Urząd wykorzystuje program monitorujący aktywność systemu w celu ochrony istotnych procesów tego systemu oraz odizolowane środowisko operacyjne w celu weryfikacji nieznanych, niezaufanych i podejrzanych aplikacji.
- Serwerownia jest odpowiednio zabezpieczona i wyposażona. Dostęp do pomieszczenia posiadają tylko osoby upoważnione.
- W procedurach wewnętrznych Jednostki określono zasady:

- przesyłania danych poza obszar przetwarzania,
- napraw, przekazania i likwidacji elektronicznych nośników informacji.

(dowód: akta kontroli str. 302-303, 314-315)

2.14 Rozliczalność działań w systemach teleinformatycznych.

Podstawa prawna: § 20 ust. 2 rozporządzenia KRI: *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;* **§ 20 ust. 3 rozporządzenia KRI:** *Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane*
z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka; **§ 20 ust. 4 rozporządzenia KRI:** *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*

Ustalenia kontroli

Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych).

System objęty kontrolą zawiera logi, w których są odnotowane działania użytkowników, zgodnie z zapisami § 20 ust. 2 i 3 rozporządzenia KRI. Logi systemu są przechowywane przez okres ponad 2 lat, wobec czego wypełniono dyspozycję § 20 ust. 4 wyżej opisanego rozporządzenia.

Zgodnie z wyjaśnieniami Informatyka w Jednostce prowadzone są działania związane z przeglądaniem logów systemu informatycznego wykorzystywanego do realizacji

zadań zleconych z zakresu administracji rządowej, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych. (dowód: akta kontroli str. 305-307)

Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 2	Nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.
Ocena obszaru kontroli	**Pozytywna**
Wpis do książki kontroli	6
Zalecenia	W związku z nie stwierdzeniem uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów nie sformułowano zaleceń.
Pouczenie	- zgodnie z art. 48 ustawy z dnia 15 lipca 2011 roku o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224) od wystąpienia pokontrolnego nie przysługują środki odwoławcze.
Podpis kierownika jednostki kontrolującej	Z upoważnienia Wojewody Zachodniopomorskiego Bartosz Brożyński I Wicewojewoda Zachodniopomorski */podpisano kwalifikowanym podpisem elektronicznym/*