Opatów, dnia 13 marca 2026 r.

S.0012.1.2026

Komisja budżetu, finansów,
rozwoju gospodarczego i promocji powiatu
w/m

W odpowiedzi na pismo z dn. 05.03.2026 r. znak: OR-II.0012.1.4.2026 dotyczące prośby o przedłożenie informacji w zakresie funkcjonowania systemu obiegu dokumentów i organizacji pracy urzędu z punktu widzenia systemu Zarządzenia Bezpieczeństwem Informacji w Starostwie Powiatowym w Opatowie informuję, co następuje:

Zasadność i konieczność wprowadzenia systemu Zarządzenia Bezpieczeństwem Informacji w Starostwie Powiatowym w Opatowie wynika z treści art. 13 ust. 1 ustawy z dnia 17 lutego 2025 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160) oraz § 19 rozporządzenia 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), zgodnie z którymi podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności oraz 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.

W celu spełnienia ww. wymogów Powiat Opatowski przystąpił do projektu „Zwiększenie poziomu cyberbezpieczeństwa Powiatu Opatowskiego”, w ramach którego zakupiono sprzęt i oprogramowanie wzmacniające bezpieczeństwo infrastruktury IT jednostek Powiatu, w tym firewalle UTM, zarządzalne przełączniki sieciowe, punkty dostępowe Wi-Fi, serwery, macierze dyskowe NAS, urządzenia UPS, oprogramowanie do backupu oraz antywirusowe z modułem EDR. Projekt przewidywał również szkolenia z zakresu cyberbezpieczeństwa dla pracowników, kadry kierowniczej i działów IT, co pozwoliło podnieść świadomość zagrożeń w cyberprzestrzeni oraz poprawić stosowanie procedur bezpieczeństwa. Ponadto realizowane były usługi wsparcia technicznego przez zewnętrznych ekspertów, którzy wspierali konfigurację zakupionych urządzeń i oprogramowania oraz przeszkolenie pracowników IT jednostek Powiatu. Całkowity koszt realizacji projektu wyniósł 849 154 zł, z czego 82% pochodziło ze środków UE, a 18% ze środków budżetu państwa, przy zerowym wkładzie własnym Powiatu Opatowskiego.

Jednym z elementów projektu było opracowaniem dokumentacji systemu zarządzania bezpieczeństwem informacji, która wprowadzona została do użytku Zarządzeniem Nr 71/2025 z dnia 23 grudnia 2025 r. w sprawie ustalenia systemu zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Opatowie. Ustalony w ten sposób System Zarządzania Bezpieczeństwem Informacji

(dalej jako: SZBI) reguluje szereg kwestii, w tym co istotne w kontekście zadanego przez tut. Komisję pytania zasady związane z bezpieczną wymianą informacji w sieci teleinformatycznej, także w zakresie korzystania z usług i aplikacji dostępnych za pośrednictwem Internetu (np. usług chmurowych) oraz poczty elektronicznej, jak również dotyczące systemu obiegu informacji w urzędzie z punktu widzenia obiegu papierowego – poniżej przedstawia się najistotniejsze kwestie:

1. W pierwszej kolejności wskazać należy, że wprowadzono klasyfikację informacji zgodnie z procedurą PBI-02 do SZBI (informacje publiczne, wewnętrzne, limitowane). Wprowadzono możliwość oznaczania zgodnie z powyższym podziałem informacji z tym, że dla informacji limitowanych wprowadzono obowiązek stosowania tego oznaczenia przez wytwórcę informacji. W szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne lub inne informacje posiadające wartość gospodarczą, informacje o środkach technicznych i organizacyjnych dotyczące sposobów zabezpieczeń kluczowych elementów zasobów informacyjnych i systemów informatycznych, w tym w szczególności dotyczące informacji prawnie chronionych, wszelkich danych, wiedzy, informacji dotyczących rozmieszczenia aktywów Powiatu, ich wykorzystywania oraz sposobów zabezpieczenia, w tym informacji związanych z rozmieszczeniem urządzeń informatycznych i telekomunikacyjnych, konfiguracji infrastruktury techniczno-systemowej (ITS) oraz stosowanych zabezpieczeń i ochrony, a także informacji pozyskanych w wyniku analizy lub przetworzenia dostarczonych informacji, których ujawienie mogłoby narazić Powiat na szkodę lub wymaga tego istotny interes publiczny lub ważny interes państwa, bez względu na formę ich utrwalenia i sposób przechowywania, okoliczności uzyskania do nich dostępu, powinny być oznaczone jako „Informacja limitowana", „Tajemnica przedsiębiorstwa". Określono również sposoby oznaczania ww. informacji oraz zasady określające sposób postępowania z danymi kategoriami informacji, rejestrowania informacji limitowanych, przeglądu klasyfikacji informacji.

2. W zakresie organizacji pracy urzędu wprowadzono również m. in. procedurę PBI-06, która porządkuje kwestie związane z zarządzaniem uprawnieniami do zasobów IT (dot. nadawania, odbierania i zawieszania uprawnień do zasobów), stosowanymi metodami i środkami uwierzytelniania oraz procedurę PBI-05, która dotyczy sposobu zgłaszania i obsługi incydentów bezpieczeństwa informacji. Procedura ta w sposób przejrzysty reguluje kwestie związane m. in. ze zgłoszeniem zdarzenia (dedykowany formularz dla pracowników zgłaszających zaistniałe incydenty), klasyfikacją zdarzeń, procedurą naprawczą i przeciwdziałaniem podobnym zdarzeniom w przyszłości.

3. Kolejno procedura PBI-11 nakłada na pracowników obowiązki w sytuacji, gdy wymieniane są informacje z podmiotami zewnętrznymi, w tym wzory zapisów dotyczących bezpieczeństwa informacji do umów lub porozumień.

4. Procedurą PBI-12 uregulowano kwestie związane z bezpieczeństwem pracy zdalnej i stosowania urządzeń mobilnych.

5. Wprowadzony System Zarządzenia Bezpieczeństwem Informacji reguluje również inne kwestie związane z codzienną pracą urzędu, takie jak podstawowe zasady bezpieczeństwa (PBI-13) oraz szereg procedur szczegółowych wymienionych w załączniku PBI-17, takie jak procedury przygotowania/dostosowania stanowiska komputerowego, procedury związane ze zmianą haseł, uwierzytelnianiem, tworzeniem kopii, bezpieczeństwa sieci informatycznej i inne.

Dzięki wprowadzonym rozwiązaniom funkcjonowanie systemu obiegu dokumentów oraz organizacja pracy w Starostwie Powiatowym w Opatowie realizowane są obecnie w sposób usystematyzowany zgodnie z zasadami Systemu Zarządzania Bezpieczeństwem Informacji. Wszystkie procesy przetwarzania, przechowywania i udostępniania informacji odbywają się w sposób kontrolowany, zapewniający poufność, integralność i dostępność danych, zgodnie z polityką bezpieczeństwa oraz obowiązującymi procedurami PBI.

Sam obieg dokumentów realizowany jest zarówno w formie elektronicznej, przy użyciu systemu EZD PUW, jak i papierowej, z zachowaniem wymogów nadzoru nad dokumentacją bezpieczeństwa oraz

klasyfikacji informacji. System EZD umożliwia rejestrację dokumentów, dekretację, kontrolę uprawnień użytkowników oraz prowadzenie historii operacji, co zapewnia pełną rozliczalność działań w urzędzie.

Podkreślić również należy, że z punktu widzenia SZBI szczególne znaczenie ma bezpieczne zarządzanie zasobami teleinformatycznymi, w tym:

- urządzeniami mobilnymi wykorzystywanymi przez pracowników, radnych oraz podmioty zewnętrzne, takimi jak komputery przenośne, tablety i smartfony, przy zastosowaniu mechanizmów kryptograficznych i zdalnego zarządzania bezpieczeństwem;
- zarządzaniem uprawnieniami do zasobów IT, obejmującym nadawanie, odbieranie, blokowanie i usuwanie kont użytkowników oraz przypisywanie minimalnych uprawnień zgodnie z zasadą wiedzy koniecznej i zasadą najmniejszych przywilejów;
- zapewnieniem bezpieczeństwa systemów teleinformatycznych poprzez monitorowanie zdarzeń, ochronę przed szkodliwym oprogramowaniem, wykonywanie kopii zapasowych danych, kontrolę logów systemowych oraz konserwację urządzeń i nośników danych.
- infrastruktura sprzętowa, w tym komputery stacjonarne, serwery, urządzenia sieciowe oraz urządzenia peryferyjne, jest eksploatowana zgodnie z przyjętymi zasadami bezpieczeństwa. Sprzęt podlega regularnej konserwacji, aktualizacji oraz kontroli w celu zapewnienia stabilności pracy systemów i ochrony przetwarzanych informacji.

Bezpieczeństwo systemów teleinformatycznych osiąga się poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, takich jak monitorowanie zdarzeń w systemach, zarządzanie oprogramowaniem, ochrona przed złośliwym oprogramowaniem, wykonywanie kopii zapasowych danych, kontrola logów systemowych oraz regularna konserwacja urządzeń i nośników danych. Wszelkie incydenty bezpieczeństwa są obsługiwane zgodnie z ww. procedurą PBI-05, zapewniając szybkie reagowanie na zagrożenia dla poufności, integralności lub dostępności informacji.

Podsumowując wprowadzone zmiany powodują, że w Starostwie wszelka dokumentacja jest gromadzona, przetwarzana i archiwizowana w sposób bezpieczny, zgodny z polityką bezpieczeństwa informacji. System EZD PUW (elektroniczny obieg dokumentów) zapewnia bezpieczny obieg dokumentów i kontrolę procedur administracyjnych, wszystkie procesy funkcjonują w istniejącym systemie, a jego funkcjonowanie jest nadzorowane przez NASK, co zapewnia zgodność z wymaganiami krajowymi dotyczącymi cyberbezpieczeństwa jednostek publicznych. Dzięki wdrożonym rozwiązaniom obieg dokumentów i organizacja pracy urzędu są realizowane w sposób spójny, bezpieczny i zgodny z wymogami SZBI, przy zapewnieniu ciągłości działania, ochrony danych i monitorowania zagrożeń w cyberprzestrzeni.

Otrzymują:
1. Adresat.
2. Aa.

Paweł Henryk Sadrak

Elektronicznie podpisany przez Paweł Henryk Sadrak
Data: 2026.03.13 11:51:49 +01'00'