Załącznik do uchwały nr 1579/438/23
Zarządu Województwa Mazowieckiego
z dnia 26 września 2023 r.

Regulamin audytu bezpieczeństwa informacji

Rozdział 1
Postanowienia ogólne

§ 1.
Zakres stosowania

1. Regulamin audytu bezpieczeństwa informacji określa:
   1) zasady przeprowadzania audytów w zakresie ochrony danych osobowych przetwarzanych w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie oraz u dostawców Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie, z którymi zawarto umowy powierzenia przetwarzania danych osobowych, oraz w zakresie zgodności z wymogami normy ISO/IEC 27001:2022;
   2) obowiązki i uprawnienia audytora podczas audytów bezpieczeństwa informacji oraz pracowników audytowanych komórek organizacyjnych Urzędu lub dostawców.
2. Audyty bezpieczeństwa informacji stanowią formę specjalistyczną audytów zintegrowanego systemu zarządzania.

§ 2.
Terminy i skróty

Terminy i skróty wykorzystywane w Regulaminie oznaczają:

1) Urząd – Urząd Marszałkowski Województwa Mazowieckiego w Warszawie;
2) ADO – Administrator danych osobowych — osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
3) Audyt BI – Audyt bezpieczeństwa informacji – audyt polegający na weryfikacji zgodności przetwarzania danych z przepisami prawa, umowami oraz regulacjami wewnątrzorganizacyjnymi, a także zgodności z wymogami normy ISO/IEC 27001:2022;
4) BBI – Biuro Bezpieczeństwa Informacji w Departamencie Organizacji w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie – komórka organizacyjna Urzędu, która prowadzi sprawy z zakresu bezpieczeństwa informacji;
5) BI – Bezpieczeństwo informacji – to zachowanie:
   - poufności, czyli zapewnienie, że dostęp do informacji mają tylko osoby upoważnione;
   - integralności, czyli zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
   - dostępności, czyli zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba;

6) Dostawca – podmiot zewnętrzny, z którym zawarto umowę w zakresie świadczenia usług lub produktów na rzecz Urzędu, w tym podmioty przetwarzające w rozumieniu art. 4 pkt 8 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
7) IOD – Inspektor Ochrony Danych;
8) Kierownik BBI – kierownik Biura Bezpieczeństwa Informacji;
9) SW-DU – Sekretarz Województwa-Dyrektor Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie;
10) ZSZ – zintegrowany system zarządzania;
11) UODO – Urząd Ochrony Danych Osobowych.

§ 3.

Rodzaje audytów

1. Audyty BI mogą być przeprowadzane jako audyty planowe lub audyty doraźne.
2. Podstawą przeprowadzania audytu planowego jest zaakceptowany przez SW-DU oraz właściwego ADO program audytów BI.
3. Podstawą przeprowadzania audytu doraźnego jest zlecenie przeprowadzenia audytu doraźnego.

§ 4.

Audytorzy

1. Audytorami przeprowadzającymi audyty BI mogą być: kierownik BBI lub pracownicy BBI, IOD, lub osoby przeprowadzające audyt na podstawie upoważnienia udzielonego przez ADO albo przez osobę przez niego upoważnioną.
2. Pracownicy BBI mają status audytorów ZSZ, nadany na mocy odpowiedniego Zarządzenia Marszałka Województwa Mazowieckiego.
3. Dopuszcza się prowadzenie audytów BI przez innych audytorów ZSZ, powołanych Zarządzeniem Marszałka Województwa Mazowieckiego.

§ 5.

Audyty planowe

1. Audyty planowe prowadzi się na podstawie rocznych programów audytów BI.
2. Roczny program audytów BI jest komplementarny do programu audytów ZSZ.
3. Roczny program audytów BI opracowuje kierownik BBI przy współudziale Pełnomocnika ds. ZSZ.
4. Roczny program audytów BI opracowuje się do 20 grudnia roku poprzedniego.
5. Po zatwierdzeniu przez SW-DU, roczny program audytów BI wymaga akceptacji właściwego ADO.
6. Roczny program audytów BI zawiera co najmniej:
   1) nazwę audytowanego departamentu/kancelarii lub dostawcy;
   2) zakres audytu;
   3) cel audytu;
   4) kryteria audytu;
   5) termin przeprowadzenia audytu.
7. Roczny program audytów BI jest publikowany na stronie intranetowej Urzędu.

8. Do zmian rocznego programu audytów BI, ust. 3 stosuje się odpowiednio.
9. Przy wyborze podmiotów audytowanych do rocznego programu audytów BI uwzględnia się w szczególności następujące kryteria:
   1) znaczenie procesów dla organizacji;
   2) poziom ryzyka bezpieczeństwa informacji oraz przetwarzania danych osobowych
   3) zaistniałe incydenty bezpieczeństwa informacji, w tym naruszenia ochrony danych osobowych;
   4) wyniki poprzednich audytów lub kontroli;
   5) jakość wpisów w *Rejestrze czynności przetwarzania*;
   6) wskazania najwyższego kierownictwa, IOD lub Pełnomocnika Marszałka Województwa ds. ZSZ do przeprowadzenia audytów;
   7) plan kontroli Prezesa UODO;
   8) zmiany w przepisach prawa, orzecznictwie, normach, decyzjach/wytycznych Prezesa UODO;
   9) dążenie do spełnienia wymagań normy ISO 27001:2022;
   10) wymogi przeglądu danych osobowych, określone w:
      a) ustawie z dnia 4 marca1994 r. o zakładowym funduszu świadczeń socjalnych;
      b) ustawie z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej,
      c) ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych;
   11) dążenie do objęcia audytami całej organizacji.

§ 6.

Audyty doraźne

1. Audyty doraźne mają charakter interwencyjny, w szczególności wynikający z potrzeby zbadania nagłych zdarzeń, na podstawie informacji otrzymanych przez IOD, kierownika BBI lub Pełnomocnika Marszałka Województwa ds. ZSZ, w szczególności w celu:
   1) zbadania określonych spraw związanych z BI, w tym ochroną danych osobowych, wynikających ze skarg lub sygnałów wpływających do Urzędu;
   2) pilnego zbadania nagłych i nieprzewidzianych zdarzeń związanych z BI.
2. Audyty doraźne prowadzi się na podstawie zlecenia wydanego przez SW-DU lub właściwego ADO.
3. Dyrektor departamentu/kancelarii, IOD, Pełnomocnik Marszałka Województwa ds. ZSZ mogą wystąpić do SW-DU z wnioskiem o przeprowadzenie audytu doraźnego wraz z uzasadnieniem.
4. W przypadku przeprowadzenia audytu doraźnego nie stosuje się § 9 ust. 1 i 2 oraz § 12 ust. 1.
5. Do przeprowadzenia audytu doraźnego stosuje się odpowiednio § 9 ust. 3-6, § 10, § 12 ust. 2-4, § 13 i § 14.

§ 7.

Sprawozdanie

Kierownik BBI przedkłada SW-DU, właściwemu ADO, Pełnomocnikowi Marszałka Województwa ds. ZSZ, Pełnomocnikowi Marszałka Województwa ds. cyberbezpieczeństwa oraz IOD roczne sprawozdanie z wykonania programu audytów BI oraz z audytów doraźnych.

§ 8.

Reagowanie na zagrożenia

1. W przypadkach stwierdzenia okoliczności wymagających podjęcia natychmiastowych działań z uwagi na zagrożenie BI, kierownik BBI podejmuje działania opisane w odpowiednim procesie w Księdze Zarządzania Procesami ZSZ, dotyczącym zarządzania incydentami związanymi z BI.
2. Postępowanie z niezgodnościami prowadzone jest zgodnie z procesem dotyczącym nadzoru nad wyrobem niezgodnym, opisanym w Księdze Zarządzania Procesami ZSZ.

Rozdział 2
Audyt prowadzony w Urzędzie

§ 9.

Organizacja audytu w Urzędzie

1. Audyt planowy w Urzędzie prowadzony jest przez co najmniej dwóch audytorów.
2. O planowanym audycie audytor powiadamia dyrektora departamentu/kancelarii z 7- dniowym wyprzedzeniem.
3. Audyt przeprowadza się w godzinach pracy Urzędu.
4. Audytorzy przed przystąpieniem do czynności audytowych mają obowiązek okazania identyfikatora, chyba że audyt prowadzony jest w formie zdalnej.
5. Audytorom w czasie wykonywania czynności audytowych może towarzyszyć inny pracownik Urzędu – w charakterze eksperta.
6. Pracownik, o którym mowa w ust. 5, w terminie wskazanym przez audytora, sporządza pisemną notatkę z przeprowadzonych czynności, którą następnie dołącza się do dokumentów audytu.

§ 10.

Uprawnienia audytorów i audytowanych w Urzędzie

1. W ramach czynności audytowych audytorzy mają prawo:
   1) wglądu do dokumentów objętych zakresem audytu, w celu weryfikacji ich zawartości oraz jeżeli zajdzie taka konieczność, do sporządzenia kopii;
   2) dostępu do wszystkich pomieszczeń departamentu/kancelarii, w celu przeprowadzenia oględzin dokumentowanych notatką z oględzin lub zdjęciami;
   3) dostępu do wszystkich systemów informatycznych departamentu/kancelarii oraz wszelkich nośników informacji, których weryfikacja jest niezbędna do przeprowadzenia audytu, w celu weryfikacji ich zawartości oraz sposobów ich zabezpieczenia;
   4) wykonywania zdjęć pomieszczeniom, dokumentom oraz innym nośnikom informacji;
   5) żądania od dyrektora lub pracownika departamentu/kancelarii ustnych lub pisemnych wyjaśnień.
2. Dyrektor departamentu/kancelarii zapewnia audytorom warunki i środki techniczne niezbędne do sprawnego przeprowadzenia audytu.
3. Pracownicy departamentu/kancelarii mają obowiązek współpracować z audytorami celem sprawnego przeprowadzenia audytu.

4. Dyrektor departamentu/kancelarii lub wyznaczony przez niego pracownik mają prawo do czynnego uczestniczenia w każdym etapie audytu.
5. W przypadku, gdy działania/zaniechania departamentu/kancelarii utrudniają realizację czynności audytowych, audytor informuje o zaistniałym stanie SW-DU oraz zawiesza prowadzenie audytu do czasu decyzji SW-DU. Audytor o fakcie zawieszenia audytu informuje także Pełnomocnika Marszałka Województwa ds. ZSZ.
6. Za działania/zaniechania, o których mowa w ust. 5, rozumie się w szczególności nieprzedstawienie do audytu dokumentów lub materiałów niezbędnych do przeprowadzenia audytu, składanie wyjaśnień uniemożliwiających jednoznaczne określenie stanu faktycznego oraz zachowanie utrudniające realizację przez audytorów czynności, o których mowa w ust. 1.

§ 11.

Dokumentacja czynności audytowych w Urzędzie

1. Audytorzy sporządzają raport z audytu planowego w terminie 30 dni od dnia zakończenia audytu, przez co rozumie się dzień realizacji ostatniej czynności audytowej realizowanej przy udziale audytowanego departamentu/kancelarii. Raport sporządza się wyłącznie w formie elektronicznej.
2. Raport, o którym mowa w ust. 1, powinien zawierać minimum:
   1) nazwę departamentu/kancelarii oraz imię i nazwisko dyrektora departamentu/kancelarii;
   2) imiona i nazwiska audytorów oraz osób biorących udział w audycie;
   3) termin przeprowadzenia audytu – datę rozpoczęcia i zakończenia audytu;
   4) zakres przedmiotowy audytu;
   5) kryteria audytu;
   6) ewentualnie stwierdzone niezgodności;
   7) ewentualne obszary do doskonalenia.
3. Kierownik BBI podpisuje raport z przeprowadzonego audytu, a następnie, po ewentualnej akceptacji SW-DU, przekazuje raport dyrektorowi departamentu/kancelarii oraz do wiadomości IOD i Pełnomocnikowi Marszałka Województwa ds. ZSZ.
4. Dyrektor departamentu/kancelarii, w terminie 7 dni od dnia otrzymania raportu, odsyła do kierownika BBI podpisany elektronicznie raport. W przypadku stwierdzenia niezgodności, dyrektor departamentu/kancelarii załącza do raportu dodatkowe wyjaśnienia dla SW-DU.
5. Do podpisanego raportu mogą być załączone zastrzeżenia o charakterze formalnym, dotyczące ustalonego stanu faktycznego.
6. Kierownik BBI opracowuje stanowisko do zgłoszonych wyjaśnień lub zastrzeżeń i przekazuje całość dokumentacji do SW-DU celem ewentualnego podjęcia decyzji o sposobie dalszego postępowania.
7. Dokumentacja związana z audytem prowadzona jest w formie elektronicznej przez BBI.

Rozdział 3
Audyt dostawców

§ 12.

Organizacja audytu dostawcy

1. Audyt planowy prowadzony jest przez co najmniej dwóch audytorów.

2. Audytor powiadamia dostawcę o planowanym audycie w terminie określonym w umowie zawartej z dostawcą lub innym instrumencie prawnym, będącym podstawą prowadzonego audytu, a jeśli termin nie został określony, co najmniej 7 dni przed rozpoczęciem audytu.
3. Audyt przeprowadza się w godzinach pracy dostawcy.
4. Audytorzy przed przystąpieniem do czynności audytowych mają obowiązek okazania legitymacji służbowej oraz upoważnienia, którego wzór stanowi załącznik do niniejszego regulaminu, a jeżeli audyt prowadzony jest w formie zdalnej – audytorzy przesyłają skany upoważnień.

§ 13.
Uprawnienia audytorów i audytowanych u dostawcy

1. W ramach czynności audytowych audytorzy mają prawo:
   1) wglądu do dokumentów regulujących zasady BI w podmiocie przetwarzającym, w szczególności: Polityki bezpieczeństwa, rejestru wszystkich kategorii czynności, rejestru umów powierzenia przetwarzania danych, rejestru naruszeń, rejestru upoważnień oraz upoważnień do przetwarzania danych osobowych, stosowanych klauzul informacyjnych, przyjętych zgód na przetwarzanie danych osobowych – wyłącznie w zakresie odnoszącym się do świadczonej przez dostawcę usługi;
   2) wglądu do dokumentów zawierających powierzone informacje, w tym w szczególności dane osobowe w celu weryfikacji ich zawartości oraz jeżeli zajdzie taka konieczność, do sporządzenia ich kopii;
   3) dostępu do pomieszczeń, w których przetwarzane są informacje związane z realizacją usługi, w celu przeprowadzenia oględzin dokumentowanych notatką z oględzin;
   4) dostępu do systemów informatycznych dostawcy, w których przetwarzane są dane osobowe powierzone przez właściwego ADO oraz wszelkich innych informacji, których weryfikacja jest niezbędna do przeprowadzenia audytu, w celu weryfikacji ich zawartości oraz sposobów ich zabezpieczenia, o ile służą do realizacji świadczonej usługi;
   5) wykonywania zdjęć pomieszczeniom, dokumentom oraz innym nośnikom informacji, w celu udokumentowania czynności, o których mowa w pkt 1-4;
   6) żądania od osób reprezentujących podmiot przetwarzający lub pracownika dostawcy ustnych lub pisemnych wyjaśnień.
2. Osoby reprezentujące dostawcę zapewniają audytorom warunki i środki techniczne niezbędne do sprawnego przeprowadzenia audytu.
3. Audytorzy są zobowiązani do zachowania poufności wszelkich informacji jakie uzyskają w trakcie prowadzonego audytu.
4. Uprawnienia określone w ust. 1 mogą być ograniczane ze względu na tajemnicę przedsiębiorstwa, jednak nie może to uniemożliwiać realizacji audytu. W przypadku wystąpienia takiego ograniczenia, audytorzy przyjmują w ww. zakresie pisemne wyjaśnienia od dostawcy.
5. Osoby reprezentujące dostawcę, u którego przeprowadzany jest audyt, lub wyznaczony przez niego pracownik mają prawo do czynnego uczestniczenia w każdym etapie audytu.
6. W przypadku, gdy działania/zaniechania dostawcy utrudniają realizację czynności audytowych, audytor informuje o zaistniałym stanie SW-DU i zawiesza prowadzenie audytu do czasu podjęcia decyzji przez SW-DU o dalszym sposobie postępowania.

7. Za działania/zaniechania, o których mowa w ust. 6, rozumie się w szczególności nieprzedstawienie do audytu dokumentów lub materiałów niezbędnych do przeprowadzenia audytu, składanie wyjaśnień uniemożliwiających jednoznaczne określenie stanu faktycznego oraz zachowanie utrudniające realizację przez audytorów czynności, o których mowa w ust. 1.

§ 14.

Dokumentacja czynności audytowych u dostawcy

1. Audytorzy sporządzają raport z audytu planowego w terminie 30 dni od dnia zakończenia audytu, przez co rozumie się dzień realizacji ostatniej czynności audytowej przy udziale dostawcy. Raport sporządza się w formie elektronicznej, chyba że umowa zawarta z dostawcą nie dopuszcza możliwości elektronicznego dostarczenia dokumentu.
2. Raport, o którym mowa w ust. 1, powinien zawierać co najmniej:
   1) nazwę dostawcy oraz imię i nazwisko osoby reprezentującej;
   2) imiona i nazwiska audytorów oraz osób biorących udział w audycie;
   3) zwięzły opis działań dostawcy w obszarze objętym audytem;
   4) termin przeprowadzenia audytu – datę rozpoczęcia i zakończenia audytu;
   5) zakres przedmiotowy audytu;
   6) opis stanu faktycznego stwierdzonego w toku przeprowadzanego audytu;
   7) ewentualnie stwierdzone niezgodności;
   8) ewentualne obszary do doskonalenia.
3. Kierownik BBI podpisuje raport z przeprowadzonego audytu, a następnie przekazuje raport do ewentualnej akceptacji SW-DU oraz do wiadomości IOD i Pełnomocnikowi Marszałka Województwa ds. ZSZ.
4. Po akceptacji raportu przez SW-DU, raport przekazuje się dostawcy.
5. W terminie 7 dni od otrzymania raportu dostawca może zgłosić do jego treści uzasadnione zastrzeżenia.
6. W przypadku zgłoszenia zastrzeżeń, o których mowa w ust. 5, kierownik BBI w terminie 7 dni przygotowuje stanowisko do zastrzeżeń, które z wykorzystaniem drogi służbowej przekazuje do SW-DU w celu ewentualnego podjęcia decyzji o dalszym sposobie postępowania.
7. Dokumentacja związana z audytem prowadzona jest w formie elektronicznej przez BBI.

METRYKA DOKUMENTU				
Nazwa	Regulamin audytu bezpieczeństwa informacji			
Opracował	Biuro Bezpieczeństwa Informacji			
Przyjął	Zastępca Dyrektora Departamentu Organizacji ds. Organizacyjnych			
Zatwierdził	Sekretarz Województwa – Dyrektor Urzędu			
Klasyfikacja	Do użytku wewnętrznego			
Historia dokumentu	Wersja	Data	Autor	Opis zmian
	1.0	26.09.2023	OR-OP-II	Utworzenie dokumentu