POLITYKA BEZPIECZEŃSTWA W RELACJACH Z PODMIOTAMI ZEWNĘTRZNYMI

Numer referencyjny dokumentu: 1.2

SPIS TREŚCI

§ 1

WSTĘP

1. Zgodnie z § 17 *Polityki Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, wprowadza się do stosowania *Politykę bezpieczeństwa w relacjach z podmiotami zewnętrznymi*, **stanowiącą dokument I poziomu SZBIiCD**.
2. Relacje UMWP z podmiotami zewnętrznymi mają charakter sformalizowany, a współpraca odbywa się w oparciu o obowiązujące przepisy prawa, *Politykę Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, niniejszą *Politykę* oraz indywidualne umowy i porozumienia.
3. Rejestry zawartych umów i porozumień prowadzone są w poszczególnych komórkach organizacyjnych UMWP przez ich kierowników lub osoby przez nich wyznaczone.
4. Celem zapewnienia ochrony aktywów informacyjnych udostępnianych podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP i/lub mającym dostęp do aktywów Urzędu oraz utrzymania ciągłości realizacji usług świadczonych przez ww. podmioty, wprowadza się niniejsze zasady i wymogi bezpieczeństwa i ciągłości działania.
5. Przedmiotowe zasady i wymogi dot. w szczególności:
   1) udostępniania aktywów informacyjnych oraz monitorowania i kontroli dostępu,
   2) przestrzegania określonych zasad i wymogów przez podmioty zewnętrzne,
   3) obowiązków podmiotów zewnętrznych w zakresie zapewnienia ochrony aktywów informacyjnych UMWP i ciągłości świadczonych usług,
   4) zgłaszania przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji i/lub ciągłości działania,
   5) uświadamiania pracowników podmiotów zewnętrznych w zakresie bezpieczeństwa informacji i ciągłości działania,
   6) postępowania z poufnymi informacjami, w tym powierzonymi podmiotom zewnętrznym danymi osobowymi,
   7) dodatkowych wymogów w zakresie utrzymania ciągłości realizacji procesów krytycznych.
6. Jednocześnie zapisy niniejszej *Polityki* stanowią punkt wyjścia do indywidualnych ustaleń i zapisów uzupełniających w umowach lub porozumieniach z podmiotami zewnętrznymi, których zakres zależy od charakteru i specyfiki współpracy.
7. W przypadku wykonywania zadań delegowanych i/lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy lub porozumienia, poza wymogami określonymi w obowiązującej w UMWP dokumentacji bezpieczeństwa i ciągłości działania, dopuszcza się stosowanie dodatkowych wymogów określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi *„zewnętrzne”* nie obniżają poziomu bezpieczeństwa pozostałych

informacji przetwarzanych w UMWP i nie generują ryzyka utraty ciągłości działania Urzędu.

8. Zapisy niniejszego dokumentu mają charakter uzupełniający do treści *Polityki Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego - dokument główny oraz* dokumentów II i III poziomu SZBIiCD, tworząc wspólnie kompleksową dokumentację bezpieczeństwa i ciągłości działania.
9. Niniejsza *Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi* podlega przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z zasadami monitorowania i aktualizacji dokumentacji bezpieczeństwa i ciągłości działania określonymi w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania*.

§ 2

WYKAZ SKRÓTÓW I DEFINICJI

1. Stosowany w treści niniejszej *Polityki* termin „podmiot zewnętrzny" (m.in. wykonawcy i kontrahenci, dostawcy produktów, materiałów i usług) oznacza wszystkich pracowników tego podmiotu, wykonujących czynności w imieniu i na rzecz UMWP i/lub mających dostęp do aktywów Urzędu w związku z realizacją zawartej umowy lub porozumienia.
2. Pozostałe stosowane w niniejszej *Polityce* definicje i skróty należy rozumieć zgodnie z *Wykazem skrótów i definicji*, stanowiącym załącznik nr 1 do *Polityki Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny.*

§ 3

ZAKRES STOSOWANIA

1. Niniejsza *Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi* określa podstawowe zasady i wymogi w zakresie współpracy z podmiotami zewnętrznymi, w tym współpracy w obszarze dostaw technologii informacyjnych i telekomunikacyjnych.
2. Podmiot zewnętrzny będący stroną zawartej umowy lub porozumienia zobowiązany jest do zapoznania podległych mu pracowników realizujących przedmiot ww. umowy lub porozumienia z zasadami ochrony aktywów informacyjnych Urzędu Marszałkowskiego Województwa Pomorskiego (UMWP), określonymi w szczególności w *Polityce Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* oraz niniejszej *Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi.*
3. Pracownicy podmiotów zewnętrznych, o których mowa w ust. 2 zobowiązani są do przestrzegania wymogów określonych w ww. *Politykach*.

§ 4

PRZYZNAWANIE DOSTĘPU DO AKTYWÓW INFORMACYJNYCH URZĘDU

1. Pracownicy podmiotów zewnętrznych, realizujący określone zadania na podstawie zawartej umowy lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych Urzędu, w tym do:
   1) informacji sklasyfikowanych w poszczególnych grupach:
      a) dane osobowe,
      b) tajemnice prawnie chronione,
      c) tajemnice Urzędu,
      d) informacje jawne,
   2) aktywów wspierających przetwarzanie ww. informacji:
      a) sprzęt (w tym komputery, nośniki informacji),
      b) oprogramowanie,
      c) sieć,
      d) personel (w tym pracownicy UMWP),
      e) lokalizacja/siedziba (w tym pomieszczenia biurowe Urzędu),
      f) organizacja (w tym procedury wewnętrzne określające zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych Urzędu),

w ograniczonym zakresie, niezbędnym do realizacji zleconych prac.

2. Przyznawanie, zmiana i odbieranie ww. dostępu do aktywów informacyjnych odbywa się zgodnie z obowiązującymi przepisami prawa, na formalny wniosek właściwego kierownika komórki organizacyjnej, odpowiedzialnego za przygotowanie i/lub realizację umowy lub porozumienia, na zasadach i w trybie określonym w *Polityce kontroli dostępu* i treści *dedykowanych Polityk dla poszczególnych grup informacji*.
3. Przyznawanie rozszerzonych uprawnień lub dodatkowych przywilejów możliwe jest po przedłożeniu stosownego uzasadnienia przez ww. kierownika i po formalnym odnotowaniu przedmiotowej zmiany.
4. Dostęp zdalny podmiotów zewnętrznych do aktywów informacyjnych Urzędu, np. w związku z wykonywaniem prac serwisowych i aktualizacji, przyznawany jest w zakresie niezbędnym do realizacji zadań i tylko pod nadzorem uprawnionych pracowników Urzędu.
5. Zasady dostępu fizycznego do budynków i pomieszczeń UMWP dla pracowników podmiotów zewnętrznych:
   1) Pracownicy podmiotów zewnętrznych mają swobodny dostęp do ogólnodostępnej strefy bezpieczeństwa obejmującej wejścia do budynków UMWP, hole, korytarze oraz wybrane pomieszczenia niestanowiące pomieszczeń ograniczonego dostępu i/lub podwyższonego poziomu bezpieczeństwa, w tym pomieszczenia użyteczności publicznej takie jak punkty obsługi klienta, poczta etc.

2) Pracownicy podmiotów zewnętrznych mogą uzyskać dostęp do strefy administracyjnej (ograniczonego dostępu), w tym pomieszczeń biurowych, w zakresie wynikającym z realizacji zadań określonych w treści zawartych umów lub porozumień i na formalny wniosek właściwego kierownika.

3) W strefie o podwyższonym poziomie bezpieczeństwa obejmującej m.in. serwerownie, pracownicy podmiotów zewnętrznych mogą przebywać tylko pod ścisłym nadzorem wybranych pracowników Departamentu Cyfryzacji (DC) tj. Generalnego Administratora Systemu Informatycznego (GASI) lub Administratora Systemu Informatycznego (ASI). Dostęp do strefy o podwyższonym poziomie bezpieczeństwa jest na bieżąco rejestrowany.

§ 5

PODSTAWOWE ZASADY BEZPIECZEŃSTWA I CIĄGŁOŚCI DZIAŁANIA W ZAKRESIE WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI

1. W uzupełnieniu do zasad i wymogów określonych w *Polityce Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, pracownicy podmiotów zewnętrznych zobowiązani są przestrzegać poniższych zasad.
2. W przypadku korzystania z budynków i pomieszczeń UMWP, pracownicy podmiotów zewnętrznych zobowiązani są do zapoznania i stosowania się do zapisów obowiązującej instrukcji przeciwpożarowej i przepisów BHP.
3. W uzasadnionych przypadkach mogą być prowadzone dodatkowe szkolenia dla pracowników podmiotów zewnętrznych z zakresu bezpieczeństwa informacji i ciągłości działania.
4. Ww. pracownicy zobowiązani są stale troszczyć się o powierzone im aktywa informacyjne oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w szczególności zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi poprzez stosowanie adekwatnych zabezpieczeń.
5. Celem zabezpieczenia aktywów, o których mowa w ust. 4, pracownicy podmiotów zewnętrznych zobowiązani są do przesyłania plików zawierających informacje chronione (m.in. dane osobowe) z wykorzystaniem sieci Internet, w tym za pośrednictwem poczty elektronicznej, w formie zaszyfrowanej. Zaszyfrowane pliki musza być przesyłane w sposób umożliwiający ich ponowne odszyfrowanie po stronie odbiorcy np. po podaniu unikalnego hasła do pliku.

   Hasło do zabezpieczonych plików należy przekazać odbiorcy innym kanałem komunikacji od użytego do przesłania danych. Za powyższe czynności odpowiedzialna jest osoba przekazująca dane.
6. Pracownikom podmiotów zewnętrznych nie wolno podejmować prób sprawdzania, testowania i omijania zabezpieczeń powierzonych im aktywów informacyjnych, w tym:

   1) samowolnie modyfikować ustawień związanych z bezpieczeństwem,

   2) świadomie wprowadzać błędnych danych,

3) podejmować prób przywłaszczenia lub rozszyfrowania informacji uwierzytelniających innych użytkowników.

7. W ramach zapewnienia poufności przetwarzanych informacji , pracownicy podmiotów zewnętrznych zobowiązani są zachować w tajemnicy przez czas nieokreślony (w trakcie jak i po zakończeniu trwania umowy lub porozumienia) informacje udostępnione im w związku z realizacją umowy lub porozumienia oraz chronić je przed ujawnieniem osobom nieuprawnionym.
8. Wymóg zachowania poufności, o którym mowa w ust. 7 obejmuje wszelkie informacje chronione, których ujawnienie mogłoby narazić UMWP na szkodę. Przedmiotowy wymóg nie dotyczy informacji, które:
   1) są jawne i ogólnodostępne,
   2) przekazane zostały podmiotowi zewnętrznemu z możliwością dalszego ujawnienia.
9. W trakcie trwania umowy lub porozumienia, podmiot zewnętrzny zobowiązuje się ponadto:
   1) do wykonania przedmiotu umowy lub porozumienia:
      a) zgodnie z wymogami prawa powszechnie obowiązującego i treścią zawartej umowy lub porozumienia,
      b) z zachowaniem najwyższej profesjonalnej staranności i przy wykorzystaniu całej posiadanej wiedzy i doświadczenia,
      c) przy wsparciu personelu posiadającego niezbędną wiedzę i umiejętności,
      d) w sposób niepowodujący przerwania lub zakłócenia ciągłości pracy Urzędu,
   2) nie zapoznawać się z dokumentami, analizami, zawartością systemu i aplikacji, dysków twardych etc., które nie są związane z przedmiotem umowy lub porozumienia,
   3) nie powielać powierzonych informacji w zakresie szerszym, niż jest to niezbędne dla realizacji przedmiotu umowy lub porozumienia, w tym nie kopiować informacji celem udostępnienia ich osobom nieuprawnionym.
10. Po zakończeniu przedmiotowej współpracy, podmiot zewnętrzny zobowiązany jest niezwłocznie, w zależności od decyzji Urzędu, zwrócić lub zniszczyć udostępnione aktywa, w tym sprzęt lub informacje przekazane mu na dowolnych nośnikach, włączając wszelkie ich kopie.

    Na pisemne polecenie Urzędu, fakt zwrotu aktywów, w tym informacji potwierdza się w formie pisemnego protokołu przekazania.

    W przypadku zniszczenia aktywów, podmiot zewnętrzny zobowiązany jest (na polecenie Urzędu) złożyć pisemne oświadczenie potwierdzające przeprowadzenie zniszczenia.
11. Dodatkowe zapisy dot. obowiązków podmiotów zewnętrznych wykonujących usługę ochrony i sprzątania w budynkach i pomieszczeniach UMWP określa dedykowana

procedura Departamentu Zamówień Publicznych i Administracji (DAZ), stanowiąca dokument III poziomu SZBIiCD.

§ 6

TREŚĆ UMÓW I POROZUMIEŃ Z PODMIOTAMI ZEWNĘTRZNYMI

1. Celem ograniczenia ryzyka związanego z dostępem podmiotów zewnętrznych do aktywów UMWP lub utratą ciągłości działania Urzędu, w treści zawieranych umów lub porozumień wprowadza się niezbędne wymogi dot. bezpieczeństwa aktywów informacyjnych i/lub utrzymania ciągłości świadczonych usług, do których przestrzegania w trakcie i po zakończeniu umowy lub porozumienia zobowiązany jest ww. podmiot zewnętrzny.
2. Podstawowy zakres wymogów, o których mowa w ust. 1 wynika wprost z obowiązujących przepisów prawa oraz dokumentacji bezpieczeństwa i ciągłości działania, w szczególności *Polityki bezpieczeństwa informacji i ciągłości działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* oraz niniejszej *Polityki*.
3. Właściwy kierownik komórki organizacyjnej, odpowiedzialny za przygotowanie i/lub realizację umowy lub porozumienia, przygotowuję adekwatne zapisy dot. bezpieczeństwa informacji i/lub ciągłości działania.
4. Zakres oraz stopień szczegółowości zapisów dot. bezpieczeństwa informacji i/lub ciągłości działania w treści umowy lub porozumienia zależy od przedmiotu i specyfiki podejmowanej współpracy oraz zidentyfikowanych zagrożeń.
5. Poza standardowymi wymogami wprost określonymi w obowiązujących przepisach prawa oraz dokumentacji bezpieczeństwa i ciągłości działania, dodatkowe zapisy dot. bezpieczeństwa informacji i ciągłości działania mogą uwzględniać np.:
   1) cel i zakres przetwarzanych informacji,
   2) wykaz osób upoważnionych do wymiany informacji i listę zatwierdzonych narzędzi do komunikacji,
   3) zakres i poziom świadczonych usług,
   4) zasady i tryb postępowania w przypadku awarii lub katastrofy (maksymalny czas reakcji, maksymalny czas naprawy) i zapewnienia ciągłości świadczenia usług i dostaw,
   5) akceptowalny poziom dostępności świadczonych usług (umowy SLA),
   6) ochronę własności intelektualnej i praw autorskich,
6. Przy zawieraniu umów z kluczowymi dostawcami usług lub produktów, niezbędnych do realizacji procesów krytycznych, tam gdzie to uzasadnione należy uwzględnić w treści umowy dodatkowe zapisy dot. utrzymania ciągłości działania i świadczenia usług na rzecz UMWP dot.:
   1) ustanowienia po stronie dostawców Planów ciągłości działania (PCD) z czasami nie dłuższymi niż czasy docelowego wznowienia działania (RTO) zidentyfikowane dla danego procesu krytycznego,
   2) wykonywania przynajmniej raz do roku testów PCD przez dostawcę,

3) ich ewentualnego uczestnictwa w testach ciągłości działania realizowanych przez Urząd,

4) umożliwienia przeprowadzenia audytów PCD u dostawcy.

W przypadku korzystania przez dostawcę z usług podwykonawców wymogi określone w pkt 1-4 dotyczą również podwykonawców.

7. Dodatkowo, w przypadku powierzenia podmiotom zewnętrznym przetwarzania danych osobowych, ww. kierownik właściwej komórki organizacyjnej UMWP przygotowuje stosowne zapisy dotyczące ochrony danych osobowych (umowa powierzenia), zgodnie z Art. 28 RODO i na zasadach określonych w *Polityce bezpieczeństwa danych osobowych*.
8. Przy okazji doskonalenia dostarczanych produktów i usług, zmiany wynikające m.in. z wprowadzenia nowych wersji dokumentacji bezpieczeństwa i ciągłości działania, wprowadzenia nowych zabezpieczeń, zmiany lokalizacji, należy - tam gdzie to niezbędne - uwzględnić w formie aneksów do już istniejących umów lub porozumień.
9. *Przykładowe standardowe zapisy dot. bezpieczeństwa informacji i ciągłości działania w umowach lub porozumieniach z podmiotami zewnętrznym*i określa załącznik nr 1 do niniejszej *Polityki*.

§ 7

MONITOROWANIE I PRZEGLĄD USŁUG ŚWIADCZONYCH PRZEZ PODMIOTY ZEWNĘTRZNE

1. Dostęp podmiotów zewnętrznych i korzystanie z aktywów informacyjnych Urzędu przez ich pracowników są nadzorowane i monitorowane, m.in. za pośrednictwem systemu monitoringu wizyjnego (CCTV).
2. Bieżący nadzór nad udostępnianiem i korzystaniem przez podmioty zewnętrzne z aktywów informacyjnych UMWP prowadzi właściwy kierownik komórki organizacyjnej lub osoba/osoby przez niego wyznaczone.
3. Ww. osoby zobowiązane są również do monitorowania czy współpracujące podmioty zewnętrzne realizują swoje zadania zgodnie z prawem i treścią zawartych umów lub porozumień, a dostarczane przez nich produkty i usługi są zgodne z przedmiotem umowy lub porozumienia oraz spełniają oczekiwania odbiorców.
4. Na wniosek UMWP, podmiot zewnętrzny zobowiązany jest przekazać informacje dotyczące postępów prac, przyczyn opóźnień lub nienależytego wykonywania zawartej umowy lub porozumienia. Informacje przekazywane są niezwłocznie w formie pisemnej.
5. W uzasadnionych przypadkach, podmiot zewnętrzny zobowiązany jest umożliwić weryfikację postępów prac bezpośrednio w swojej siedzibie w trybie postępowania sprawdzającego (audytu bezpieczeństwa).
6. Przedmiotowe zapisy dot. monitorowania i przeglądu usług świadczonych przez podmioty zewnętrzne mogą zostać doszczegółowione w treści zawartych umów lub porozumień (ewentualnie w aneksach do już istniejących umów lub porozumień).

§ 8

ZGŁASZANIE PRZYPADKÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI PRZEZ PODMIOTY ZEWNĘTRZNE

1. Osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu, w przypadku zaistnienia okoliczności mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji w UMWP i/lub utraty ciągłości działania, zobowiązani są niezwłocznie poinformować o szczegółach i charakterze zdarzenia kierownika Referatu Bezpieczeństwa Informacji w Departamencie Organizacji (kierownika DO-B) lub pracownik DO-B przez niego wskazanego.
2. Zgłoszenie, o którym mowa w ust. 1, należy przesłać drogą mailową na adres incydent@pomorskie.eu, podając dane kontaktowe, okoliczności oraz czas wystąpienia zdarzenia, wskazującego na naruszenie lub próbę naruszenia (można skorzystać z *Formularza zgłoszenia naruszenia bezpieczeństwa informacji i ciągłości działania*, którego wzór stanowi załącznik nr 2 do niniejszej *Polityki*)
3. W uzasadnionych przypadkach dopuszcza się dokonanie przedmiotowego zgłoszenia w innym trybie np. telefonicznie na numer 58 326 85 18, 58 326 87 52 lub 58 326 89 71.
4. Próby/przypadki nieautoryzowanego dostępu do aktywów informacyjnych UMWP są identyfikowane jako incydenty związane z bezpieczeństwem informacji.
5. Po powzięciu informacji o okolicznościach mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji i/lub utracie ciągłości działania, dalsze postępowanie, w tym obsługa i wyjaśnienie przyczyn incydentu związanego z bezpieczeństwem informacji, odbywa się zgodnie z *Procedurą obsługi i postepowania z incydentami związanymi z bezpieczeństwem informacji i utratą ciągłością działania*, stanowiącą załącznik do *Polityki zarządzania incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania*.
6. Naruszenie postanowień umowy, porozumienia lub wymogów obowiązującej dokumentacji bezpieczeństwa i ciągłości działania przez podmiot zewnętrzny stanowi podstawę do odstąpienia od umowy lub porozumienia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynikał z zawartej umowy lub porozumienia.
7. Z tytułu działań podmiotów zewnętrznych i jego przedstawicieli, niezgodnych z przepisami prawa powszechnie obowiązującego (w tym dot. niewłaściwego przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
    1) kodeksie pracy,
    2) kodeksie cywilnym,
    3) kodeksie karnym,
    4) RODO oraz ustawie o ochronie danych osobowych.

§ 9

ZASADY WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

1. Poza współpracą z tytułu zawartych umów i porozumień, z uwagi na wymogi prawa powszechnie obowiązującego, celem zapewnienia kompleksowej ochrony przetwarzanych informacji i utrzymania ciągłości działania Urzędu, w tym ochrony przed cyberzagrożeniami, wymiany wiedzy i doświadczeń oraz wsparcia procesu zarządzania zdarzeniami, w tym incydentami związanymi z bezpieczeństwem informacji i ciągłością działania, pracownicy UMWP współpracują z wybranymi instytucjami, organizacjami oraz podmiotami sektora publicznego i prywatnego.
2. W ramach przedmiotowej współpracy, w uzasadnionych przypadkach, w szczególności:
   1) w przypadku wybranych incydentów o priorytecie wysokim,
   2) w przypadku incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny,
   3) w przypadku incydentów noszących znamiona przestępstwa,

   informacja o incydencie przekazywana jest do właściwych podmiotów zewnętrznych, w tym:
   a) organów ścigania w przypadku incydentów wyczerpujących znamiona przestępstwa (np. przestępstwa przeciwko ochronie informacji wskazane w Kodeksie Karnym),
   b) Agencji Bezpieczeństwa Wewnętrznego,
   c) właściwych zespołów reagowania na incydenty bezpieczeństwa komputerowego – w tym CSIRT NASK.
3. Współpraca z organem nadzorczym - Prezesem Urzędu Ochrony Danych Osobowych prowadzona jest w obszarze ochrony danych osobowych, w tym wymiany doświadczeń i stałego podnoszenia wiedzy pracowników UMWP.
4. Przypadki naruszenia ochrony danych osobowych prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych są niezwłocznie zgłaszane organowi nadzorczemu (Prezesowi UODO), na zasadach i w trybie szczegółowo określonym w obowiązującej w UMWP *Procedurze obsługi i postępowania z incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania.*

Załącznik nr 1 Przykładowe standardowe zapisy dot. bezpieczeństwa informacji i ciągłości działania w umowach lub porozumieniach z podmiotami zewnętrznymi

§ …

BEZPIECZEŃSTWO INFORMACJI i CIĄGŁOŚĆ DZIAŁANIA

1. W związku z realizacją niniejszej Umowy/Porozumienia*, Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* będący stroną zawartej Umowy/Porozumienia* zobowiązany jest do zapewnienia bezpieczeństwa informacji przetwarzanych w związku jej/jego* realizacją, ochrony pozostałych udostępnionych mu aktywów Urzędu Marszałkowskiego Województwa Pomorskiego (UMWP)/Zamawiającego, wspierających przetwarzanie tych informacji, w szczególności do zapewnienia ich poufności, integralności oraz dostępności oraz do zapewnienia ciągłości realizacji usług świadczonych na rzecz Urzędu.
2. Ww. Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* zobowiązuje się do wykonania przedmiotu Umowy/Porozumienia* zgodnie z przepisami prawa powszechnie obowiązującego oraz do zapoznania się przed jej podpisaniem i przestrzegania wymogów w zakresie bezpieczeństwa informacji i ciągłości działania określonych w *Polityce Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* oraz dedykowanej *Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi*, dostępnych w Biuletynie Informacji Publicznej Urzędu Marszałkowskiego Województwa Pomorskiego (*bip.pomorskie.eu*), w zakładce *Bezpieczeństwo Informacji*.
3. Podmiot, o którym mowa w ust. 1 i 2, w ramach niniejszej Umowy/Porozumienia* zobowiązuje się w szczególności:
   1) stale troszczyć się o powierzone mu informacje i aktywa wspierające ich przetwarzanie oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w tym zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnionym udostępnieniem, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi,
   2) korzystać z powierzonych mu informacji i aktywów wspierających ich przetwarzanie, zgodnie z oraz wyłącznie do celów wynikających z zapisów zawartej Umowy/Porozumienia*,
   3) przesyłać informacje chronione z wykorzystaniem sieci Internet w formie zaszyfrowanej,
   4) nie powielać, w tym nie kopiować informacji chronionych, udostępnionych i opracowanych w trakcie Umowy/Porozumienia* w zakresie szerszym, niż jest to potrzebne do jej/jego* realizacji,
   5) informować Zamawiającego o każdym podejrzeniu naruszeniu bezpieczeństwa informacji i/ lub utraty ciągłości działania Urzędu,
   6) niezwłocznie po zakończeniu niniejszej Umowy/Porozumienia*, trwale usunąć i/lub zniszczyć informacje chronione przetwarzane w ramach jej/jego* realizacji, chyba że obowiązek ich dalszego przetwarzania wynika wprost z przepisów prawa powszechnie obowiązującego.

4. Jednocześnie Zleceniobiorca/Wykonawca/Podmiot zewnętrzny* potwierdza, że pracownicy bezpośrednio realizujący przedmiot niniejszej Umowy/Porozumienia* zostali zapoznani i zobowiązani do przestrzegania przedmiotowych wymogów w zakresie bezpieczeństwa informacji i ciągłości działania.

** niepotrzebne skreślić*

FORMULARZ ZGŁOSZENIA NARUSZENIA BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA nr ……./rok[1]

1. Data i godzina zgłoszenia			
2. Źródło zgłoszenia			
2.1 Imię i nazwisko Zgłaszającego			
2.2 Stanowisko		2.3 Numer telefonu/adres email (służbowy)	
2.5 Nazwa podmiotu[2]			
3. Opis potencjalnego naruszenia bezpieczeństwa informacji/ utraty ciągłości działania			
Proszę pokrótce opisać okoliczności oraz czas wystąpienia zdarzenia, wskazującego na naruszenie lub próbę naruszenia bezpieczeństwa informacji / utraty ciągłości działania			

[1] Uzupełnia kierownik DO-B lub osoba przez niego wskazana

[2] W przypadku zgłoszeń od zleceniobiorców oraz innych i podmiotów zewnętrznych wykonujących czynności w imieniu i na rzecz UMWP i/lub mających dostęp do aktywów informacyjnych Urzędu