Ministerstwo Cyfryzacji

Narodowe Standardy Cyberbezpieczeństwa

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)

v. 2.00 – …… 2025

ul. Królewska 27I 00-060 Warszawa I tel.: +48 22 250 01 10 I tel.: +48 22 250 28 85 I e-mail: mc@mc.gov.pl www.mc.gov.pl
Ministerstwo Cyfryzacji

Spis treści

1. Wprowadzenie

Chmura obliczeniowa to technologia rozproszonego przetwarzania danych, w której skalowalne zasoby informacyjne (infrastruktura, platforma aplikacyjna i oprogramowanie) udostępniane są jako usługi dla wielu odbiorców organizacyjnych i indywidualnych.

Na chmurę obliczeniową składają się usługi teleinformatyczne dostosowywane dynamicznie do potrzeb i udostępniane w rozliczalny sposób za pośrednictwem sieci, z wykorzystaniem bezpiecznych protokołów sieciowych. Korzystanie z usług chmur obliczeniowych możliwe jest za pomocą interfejsów oferowanych przez dostawców usług.

Technologie chmur obliczeniowych wprowadzają nowe modele przetwarzania danych, niezależne od miejsca ich przechowywania – dlatego chmura obliczeniowa to nie miejsce tylko model przetwarzania.

1.1 Przeznaczenie, cel i odbiorcy dokumentu

Dokument „Standardy Cyberbezpieczeństwa Chmur Obliczeniowych" został opracowany w ramach zbioru Narodowych Standardów Cyberbezpieczeństwa, przywołanego w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024[1].

Opracowanie Narodowych Standardów Cyberbezpieczeństwa jest realizacją celu szczegółowego 2 – *Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty*.

[1] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 - http://monitorpolski.gov.pl/mp/2019/1037/1

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) stanowią zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych w ramach inicjatywy Wspólna Infrastruktura Informatyczna Państwa (WIIP)[2].

Wśród strategicznych kierunków, jakie realizuje inicjatywa WIIP są m.in:

- podniesienie poziomu bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej;
- trwałe obniżenie kosztów stałych przetwarzania danych;
- podniesienie efektywności wydatkowania środków w projektach zawierających elementy infrastruktury IT;
- skrócenie czasu realizacji nowych przedsięwzięć informatycznych przez szybsze udostępnianie wymaganej infrastruktury IT;
- ograniczenie zjawiska wielokrotnego gromadzenia tych samych danych w środowiskach informatycznych oraz zniesienie barier technologicznych w przypadku rejestrów publicznych;
- upowszechnienie modelu przetwarzania w chmurach obliczeniowych, jako głównego sposobu realizacji systemów teleinformatycznych państwa (w tym również zmiana technologii wytwarzania oprogramowania).

Ważnym elementem inicjatywy WIIP jest opracowanie klasyfikacji systemów teleinformatycznych[3] oraz wdrożenie jednolitych standardów bezpieczeństwa infrastruktury przetwarzania danych, które umożliwią migrację systemów i danych do modelu przetwarzania w chmurze obliczeniowej.

Działania w ramach inicjatywy WIIP są również elementem budowy krajowego systemu cyberbezpieczeństwa[4].

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych określają wymagania, jakie muszą spełnić:

- podmioty administracji rządowej zarządzające Centrami Przetwarzania Danych (CPD), w celu ich przyłączenia do Rządowego Klastra Bezpieczeństwa (RKB) lub włączenia do wspólnych zasobów Rządowej Chmury Obliczeniowej (RChO).
- podmioty wskazane w §6 ust. 1 uchwały WIIP planujące wykorzystanie lub korzystające z rządowych i/lub publicznych usług przetwarzania w modelach chmur obliczeniowych.

[2] Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa - http://monitorpolski.gov.pl/mp/2019/862/1 z późn. zm. https://monitorpolski.gov.pl/MP/rok/2020/pozycja/403 i https://monitorpolski.gov.pl/MP/rok/2024/pozycja/908.

[3] Klasyfikacja zawarta została w załączniku nr 2 do uchwały ws. inicjatywy WIIP w brzmieniu nadanym nowelizacją uchwały z 2024 r. https://monitorpolski.gov.pl/MP/rok/2024/pozycja/908.

[4] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U z 2024 r. poz. 1077 z późn. zm.).

- dostawcy usług chmur obliczeniowych w ramach Publicznej Chmury Obliczeniowej (PChO).

Odbiorcami Standardów Cyberbezpieczeństwa Chmur Obliczeniowych są:

- publiczni i komercyjni dostawcy usług chmurowych dla administracji publicznej,
- jednostki administracji publicznej planujące wykorzystanie lub korzystające z rządowych i/lub publicznych usług przetwarzania w modelach chmur obliczeniowych.

Przetwarzanie w modelach chmur obliczeniowych opiera się na założeniu wysokiego poziomu standaryzacji sprzętu, oprogramowania i usług, których szczegółów implementacyjnych odbiorca zwykle nie zna. W związku z tym wymagany jest szczególnie wysoki poziom zaufania do dostawców usług w chmurach obliczeniowych.

Istnieją różne narodowe i branżowe standardy wymagań oraz certyfikacji bezpieczeństwa dla usług w chmurach obliczeniowych. Z tego powodu odbiorcy usług chmur obliczeniowych mają trudności z przeglądem i porównywaniem zakresu oraz poziomu bezpieczeństwa usług oferowanych przez różnych dostawców. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych mają stanowić pomoc dla jednostek administracji publicznej planujących skorzystanie z modelu przetwarzania danych w chmurach obliczeniowych, upraszczając proces wyboru dostawcy, zakresu usług i oceny cyberbezpieczeństwa środowiska przetwarzania.

2. Struktura Standardów Cyberbezpieczeństwa Chmur Obliczeniowych

Zakres usług oferowanych w ramach modeli chmur obliczeniowych obejmuje całe spektrum technologii informacyjnych, w szczególności infrastrukturę (np. moc obliczeniowa, pamięć masowa), platformy aplikacyjne (np. repozytoria aplikacji), oprogramowanie i usługi bezpieczeństwa.

Do zdefiniowania wymagań bezpieczeństwa dla modeli chmur obliczeniowych niezbędne jest wprowadzenie standaryzacji definicji atrybutów bezpieczeństwa informacji oraz poziomów potencjalnego wpływu na bezpieczeństwo informacji (Kategorie Bezpieczeństwa) – **zawiera je rozdział 3.**

Proces wyboru optymalnego modelu chmury obliczeniowej powinien w szczególności uwzględniać analizę ryzyka z punktu widzenia atrybutów bezpieczeństwa (poufności, integralności i dostępności) oraz klasyfikacji systemu (m.in. jego wpływu na realizowane zadania statutowe) – **proces ten został opisany w rozdziale 4.**

Dostawcy usług w modelach chmur obliczeniowych są odpowiedzialni za zaprojektowanie, opis, wdrożenie i skuteczne działanie zabezpieczeń organizacyjnych i technicznych spełniających wymagania bezpieczeństwa – **wymagania te zostały opisane w rozdziale 5.**

Usługi przetwarzania w modelach chmur obliczeniowych stanowią element krajowego systemu cyberbezpieczeństwa stąd konieczne jest dostosowanie do zasad i wymagań zdefiniowanych w ustawie o krajowym systemie cyberbezpieczeństwa oraz rozporządzeń do tej ustawy, w szczególności regulujących kwestie realizacji usług z zakresu cyberbezpieczeństwa oraz zgłaszania incydentów – **tym zagadnieniom poświęcony jest rozdział 6.**

W załącznikach do Standardów Cyberbezpieczeństwa Chmur Obliczeniowych zawarto następujące informacje:

- Załącznik 1 – Wykaz przepisów prawnych, przywoływanych norm krajowych i międzynarodowych,
- Załącznik 2 – Słownik pojęć,
- Załącznik 3 – Wykaz skrótów,
- Załącznik 4 – Podstawowe Wymagania Bezpieczeństwa – macierz zabezpieczeń,
- Załącznik 5 – Katalog zabezpieczeń.

3. Atrybuty bezpieczeństwa, Kategorie Bezpieczeństwa i Poziomy Wymagań Bezpieczeństwa SCCO

3.1 Atrybuty bezpieczeństwa (poufność, integralność, dostępność) i Kategorie Bezpieczeństwa

Atrybuty bezpieczeństwa uwzględniają zagrożenia w zakresie poufności, integralności i dostępności[5].

Zgodnie z FIPS 199:

- **poufność** - zachowanie autoryzowanych ograniczeń w dostępie i ujawnianiu informacji, w tym środki ochrony prywatności i informacji o zastrzeżonym dostępie. Utrata poufności to nieuprawnione ujawnienie informacji.
- **integralność** - zabezpieczenie przed niewłaściwą modyfikacją lub zniszczeniem informacji; obejmuje zapewnienie niezaprzeczalności i autentyczności informacji. Utrata integralności to nieautoryzowana modyfikacja lub zniszczenie informacji. Należy zauważyć, że nieuprawnione zniszczenie informacji spowoduje utratę dostępności tych informacji.
- **dostępność** - zapewnienie terminowego i niezawodnego dostępu do informacji i ich wykorzystywania. Utrata dostępności oznacza zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego.

Zgodnie z uchwałą WIIP wymaga się od odbiorców usług chmur obliczeniowych, aby klasyfikowali swoje systemy informatyczne **uwzględniając łącznie potencjalny wpływ** na

[5] NIST FIPS Publication 199.

bezpieczeństwo przetwarzanych danych, wynikający z konieczności zapewnienia poufności, integralności i dostępności informacji.

Bezpośredni wpływ na kategoryzację systemu teleinformatycznego ma najwyższa wartość spośród oszacowanych atrybutów bezpieczeństwa.

Ogólny wzór wyznaczania kategoryzacji bezpieczeństwa (SC [6]) systemu teleinformatycznego:

System teleinformatyczny SC = {(poufność, wpływ), (integralność, wpływ), (dostępność, wpływ)},

gdzie dopuszczalne wartości potencjalnego wpływu są niskie, umiarkowane lub wysokie, zgodnie z Tabelą 1.

Tabela 1. Macierz – atrybuty bezpieczeństwa i kategorie potencjalnego wpływu na bezpieczeństwo

	Poziom potencjalnego wpływu na bezpieczeństwo(Kategoria Bezpieczeństwa)		
Atrybuty bezpieczeństwa	**Niski (L)**	**Umiarkowany (M)**	**Wysoki (H)**
Poufność - zachowanie autoryzowanych ograniczeń w dostępie i ujawnianiu informacji, w tym środki ochrony prywatności i informacji o zastrzeżonym dostępie	Nieuprawnione ujawnienie informacji będzie miało **ograniczony** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieuprawnione ujawnienie informacji będzie miało **poważny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieuprawnione ujawnienie informacji będzie miało **silny lub katastrofalny** niekorzystny wpływ na operacje organizacyjne, aktywa organizacyjne lub osoby fizyczne.
Integralność - zabezpieczenie przed niewłaściwą modyfikacją lub zniszczeniem informacji; obejmuje zapewnienie niezaprzeczalności i autentyczności informacji	Nieautoryzowana modyfikacja lub zniszczenie informacji będzie miała **ograniczony** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieautoryzowana modyfikacja lub zniszczenie informacji może miała **poważny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieautoryzowana modyfikacja lub zniszczenie informacji będzie miała **silny lub katastrofalny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.
Dostępność - zapewnienie terminowego i niezawodnego dostępu do informacji i ich wykorzystywania	Zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało **ograniczony** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało **poważny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało **silny lub katastrofalny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.

Przy określaniu poziomu potencjalnego wpływu na bezpieczeństwo tj. ustalaniu, czy niekorzystny wpływ będzie ograniczony, poważny, silny lub katastrofalny, należy brać pod

[6] ang. Security Categorization

uwagę kontekst i specyfikę organizacji, rodzaj przetwarzanych danych, a pomocniczo można posłużyć się przepisami ustawy o krajowym systemie cyberbezpieczeństwa w zakresie incydentów oraz rozporządzeniem wykonawczym do tej ustawy w sprawie progów uznania incydentu za poważny[7].

3.2 Poziomy wymagań bezpieczeństwa SCCO determinujące stosowanie poszczególnych modeli chmur obliczeniowych

Poziomy Wymagań Bezpieczeństwa SCCO determinujące stosowanie poszczególnych modeli chmur obliczeniowych są określane przez korelację:

1) wrażliwości lub poziomu poufności informacji (np. publicznych, urzędowych, niejawnych itp.), które mają być przechowywane oraz przetwarzane w środowisku dostawcy usług chmur obliczeniowych;
2) poziomu potencjalnego wpływu zdarzenia, które powoduje utratę poufności, integralności lub dostępności tych informacji.

Kategoryzacja bezpieczeństwa systemu teleinformatycznego ma bezpośredni wpływ na określenie Poziomu Wymagań Bezpieczeństwa determinującego wybór modelu chmur obliczeniowych - RChO/PChO, chmura prywatna oraz dobór odpowiednich zabezpieczeń bazowych i rozszerzonych

Kategoryzacji systemu teleinformatycznego dokonuje jego gestor na podstawie analizy ryzyka przeprowadzonej w udokumentowanym procesie szacowania ryzyka.

Nadrzędnym zadaniem odbiorców SCCO podczas przetwarzania informacji w Chmurze obliczeniowej jest zapewnienie bezpieczeństwa przetwarzanych informacji oraz zgodności sposobu i zakresu tego przetwarzania z obowiązującymi przepisami prawa. Zapewnienie bezpieczeństwa przetwarzanych informacji powinno być nadrzędnym celem i zadaniem odbiorców SCCO. W zależności od modelu przetwarzania w chmurze obliczeniowej ta odpowiedzialność kształtuje się w różny sposób, co powinny uwzględniać m.in. umowy o świadczenie usług przetwarzania w chmurze.

Poziomy Wymagań Bezpieczeństwa SCCO:

- Poziom SCCO1: informacje inne niż prawnie chronione,
- Poziom SCCO2: informacje prawnie chronione,
- Poziom SCCO 3: informacje niejawne o maksymalnej klauzuli „zastrzeżone” lub równoważnej klauzuli międzynarodowej,
- Poziom SCCO4: informacje niejawne

W tabeli poniżej przedstawiono rekomendacje przetwarzania poszczególnych kategorii informacji z wykorzystaniem usług chmurowych, określonych w Poziomach Wymagań Bezpieczeństwa SCCO.

[7] Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. z 2018 r. poz. 2180).

POZIOM WYMAGAŃ BEZPIECZEŃSTWA SCCO	WYMAGANE ZABEZPIECZENIA DLA CHMURY OBLICZENIOWEJ	CENTRA PRZETWARZANIA DANYCH	Możliwość przetwarzania w chmurze
Poziom SCCO 1: Informacje inne niż prawnie chronione	Zabezpieczenia bazowe na poziomie niskim / umiarkowanym potencjalnego wpływu na atrybuty bezpieczeństwa	Przetwarzanie dozwolone w centrach danych alokowanych poza Polską. Rekomendowane CPD na terenie EOG.	1. Publiczna Chmura Obliczeniowa. 2. Rządowa Chmura Obliczeniowa i Rządowy Klaster Bezpieczeństwa 3. Chmura prywatna
Poziom SCCO 2: Informacje prawnie chronione	Zabezpieczenia bazowe na poziomie umiarkowanym/wysokim + zabezpieczenia rozszerzone o ile są wymagane	Przetwarzanie dozwolone w centrach przetwarzania danych alokowanych na terenie UE. Dopuszcza się centra przetwarzania na terenie EOG jeżeli respektowane jest prawo UE. Dla informacji/systemów o kategoriach bezpieczeństwa na poziomie wysokim dla atrybutów bezpieczeństwa: poufność i integralność należy w pierwszej kolejności wykorzystywać centra danych na terenie RP.	1. Publiczna Chmura Obliczeniowa 2. Rządowa Chmura Obliczeniowa i Rządowy Klaster Bezpieczeństwa 3. Chmura prywatna
Poziom SCCO 3: Informacje niejawne o maksymalnej klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej	Zabezpieczenia bazowe na poziomie wysokim + zabezpieczenia rozszerzone + wymagania dla ochrony informacji niejawnych właściwe do klauzuli przetwarzania informacji niejawnych	Przetwarzanie dozwolone wyłącznie w centrach danych na terenie RP, **jeżeli** z analizy ryzyka i systemu zarządzania bezpieczeństwem, w szczególności z powodu braku dostępu do informacji niejawnych o maksymalnej klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej przez personel CPD, jednoznacznie wynika, że w celu zachowania m.in. odpowiedniego poziomu suwerenności danych nie jest możliwe korzystanie z usług chmurowych dostawców komercyjnych. W pozostałych przypadkach dopuszczalne jest przetwarzanie w centrach przetwarzania danych alokowanych na terenie UE. Dopuszcza się centra przetwarzania na terenie EOG jeżeli respektowane jest prawo UE. W pierwszej kolejności należy wykorzystywać centra danych na terenie RP.	1. Publiczna Chmura Obliczeniowa 2. Rządowa Chmura Obliczeniowa i Rządowy Klaster Bezpieczeństwa 3. Chmura prywatna + SOC (własny SOC lub usługa SOC as a Service) - po dokonaniu akredytacji systemu teleinformatycznego zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych i uzyskaniu zgody wyrażonej przez Służbę Kontrwywiadu Wojskowego.
Poziom SCCO 4: Informacje niejawne	Zabezpieczenia bazowe na poziomie wysokim + zabezpieczenia rozszerzone wynikające ze Szczególnych Wymagań Bezpieczeństwa + wymagania dla ochrony informacji niejawnych właściwe do klauzuli przetwarzanych informacji niejawnych	Przetwarzanie w centrach danych rozwijanych w ramach systemów teleinformatycznych akredytowanych do przetwarzania informacji niejawnych o określonej klauzuli tajności zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.	Środowiska on-premise lub chmura prywatna rozwijane w ramach systemów teleinformatycznych akredytowanych do przetwarzania informacji niejawnych o określonej klauzuli tajności zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

3.2.1. Poziom SCCO1: Informacje inne niż prawnie chronione

Poziom SCCO1 obejmuje wszystkie dane przeznaczone do publicznego udostępnienia – bez prawnych wymagań dotyczących zachowania poufności (np. publiczne strony internetowe). Obejmuje również niektóre informacje wymagające minimalnej kontroli dostępu.

Dostęp do usług odbywa się przez Internet i/lub za pośrednictwem logicznie wydzielonych usług transmisji danych.

Poziom SCCO1 obejmuje informację publiczną, która w szczególności:

- nie jest informacją prawnie chronioną,
- może posiadać ograniczenia związane z prawem autorskim.

Konsekwencje ujawnienia informacji innych niż prawnie chronione:

- ujawnienie informacji może mieć ograniczony lub poważny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne;

- nieautoryzowana modyfikacja lub zniszczenie informacji będzie miało ograniczony lub poważny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne;
- zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało ograniczony lub poważny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.

Poziom SCCO1 obsługuje informacje dla których zabezpieczenia bazowe zostały określone na poziomie niskim/umiarkowanym w zakresie potencjalnego wpływu na atrybuty bezpieczeństwa.

Jednostki administracji publicznej mogą przetwarzać informacje na poziomie SCCO1 z wykorzystaniem usług publicznych chmur obliczeniowych.

3.2.2. Poziom SCCO2: Informacje prawnie chronione

Poziom SCCO2 obejmuje informacje istotne dla realizacji działań statutowych instytucji administracji publicznej, udostępniane m.in. na podstawie porozumień o zachowaniu poufności.

Poziom SCCO2 obejmuje informacje, które w szczególności:

- zawierają dane osobowe podlegające ochronie ustawowej,
- zawierają tajemnicę przedsiębiorcy, w tym tajemnice branżowe/instytucjonalne podlegające prawnej ochronie,
- mają charakter wrażliwych, prawnie chronionych informacji i danych referencyjnych krajowych rejestrów - określonych w odrębnych przepisach (w tym dane o kluczowym znaczeniu dla bezpieczeństwa publicznego);
- wymagają jednoznacznego oznaczenia jako informacje o ograniczonym dostępie, w szczególności których nieuprawnione ujawnienie może obniżać skuteczność zabezpieczeń stosowanych w systemach administracji rządowej.

Konsekwencje ujawnienia informacji:

- negatywne konsekwencje nieupoważnionego dostępu związane są z naruszeniem przepisów dot. ochrony informacji prawnie chronionych, w szczególności danych osobowych, tajemnic zawodowych i służbowych, tajemnicy przedsiębiorcy i co za tym idzie, mogą wywołać określone ustawowe sankcje (np. art. 69 i 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, art. 23 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji).
- nieuprawnione ujawnienie informacji będzie miało poważny lub silny lub katastrofalny niekorzystny wpływ na operacje organizacyjne, aktywa organizacyjne lub osoby fizyczne.
- nieautoryzowana modyfikacja lub zniszczenie informacji będzie miała poważny lub silny lub katastrofalny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.
- zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało poważny lub silny lub katastrofalny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.

Poziom SCCO2 obsługuje informacje dla których zabezpieczenia bazowe zostały określone na poziomie umiarkowanym/wysokim w zakresie potencjalnego wpływu na atrybuty bezpieczeństwa.

Jednostki administracji publicznej mogą przetwarzać informacje ma poziomie SCCO2 z wykorzystaniem usług publicznych chmur obliczeniowych pod warunkiem, że przetwarzanie odbywa się w centrach danych alokowanych na terenie UE lub EOG, jeżeli respektowane jest prawo UE. Dla informacji/systemów o kategoriach bezpieczeństwa na poziomie wysokim dla atrybutów poufność i integralność należy w pierwszej kolejności wykorzystywać centra danych na terenie RP.

Jeżeli z analizy ryzyka i systemu zarządzania bezpieczeństwem jednoznacznie wynika, że w celu zachowania m.in. suwerenności danych czy też kontroli nad personelem technicznym nie można korzystać z usług chmurowych dostawców komercyjnych, przetwarzanie dozwolone jest wyłącznie w centrach danych na terenie RP w ramach RChO + Rządowego Klastra Bezpieczeństwa lub w ramach Chmury prywatnej.

3.2.3. Poziom SCCO3: Informacje niejawne o maksymalnej klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej

Poziom SCCO3 obejmuje informacje niejawne o maksymalnej klauzuli „zastrzeżone" klasyfikowane zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych lub równoważnej klauzuli międzynarodowej np. „NATO Restricted". Poziom SCCO3 zawiera informacje o kluczowym znaczeniu dla bezpieczeństwa publicznego, w tym bezpieczeństwa państwa.

Konsekwencje ujawnienia informacji:

- negatywne konsekwencje nieupoważnionego dostępu związane są w szczególności z naruszeniem ustawy o ochronie informacji niejawnych co oznacza, że nieuprawnione ujawnienie przedmiotowych informacji może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.
- nieuprawnione ujawnienie informacji będzie miało silny lub katastrofalny niekorzystny wpływ na operacje organizacyjne, aktywa organizacyjne lub osoby fizyczne.
- nieautoryzowana modyfikacja lub zniszczenie informacji będzie miała silny lub katastrofalny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.
- zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało silny lub katastrofalny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.

Przetwarzanie danych przez jednostki administracji publicznej jest dozwolone wyłącznie w centrach danych na terenie RP, jeżeli z analizy ryzyka i systemu zarządzania bezpieczeństwem, w szczególności z powodu braku dostępu do informacji niejawnych o maksymalnej klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej przez personel CPD, jednoznacznie wynika, że w celu zachowania m.in. odpowiedniego poziomu suwerenności danych nie jest możliwe korzystanie z usług chmurowych dostawców komercyjnych. W pozostałych przypadkach dopuszczalne przetwarzanie w centrach przetwarzania danych alokowanych na terenie UE. Dopuszcza się centra przetwarzania na terenie EOG jeżeli respektowane jest prawo UE. Należy uwzględniać wymagania dla ochrony informacji niejawnych właściwych do klauzuli przetwarzanych informacji niejawnych. W pierwszej kolejności należy wykorzystywać centra danych na terenie RP.

3.2.4. Poziom SCCO 4: Informacje niejawne

Obejmuje informacje klasyfikowane jako niejawne zgodnie z Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych z wyłączeniem informacji niejawnych o maksymalnej klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej dla których Uchwała WIIP przewiduje możliwość skorzystania z usług chmurowych w ramach RChO lub PChO.

Takie informacje mogą być przetwarzane w środowiskach on-premise lub w chmurze prywatnej rozwijanych w ramach systemów teleinformatycznych akredytowanych do przetwarzania informacji niejawnych o określonej klauzuli tajności zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

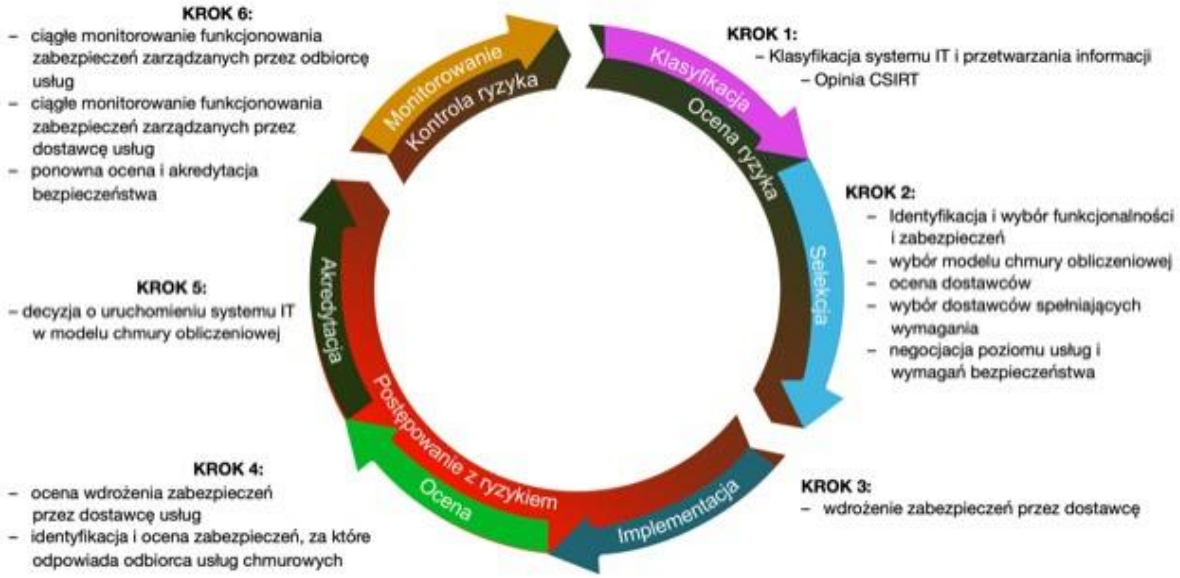
4. Proces przygotowania do przetwarzania informacji w modelach chmur obliczeniowych

Przetwarzanie informacji w modelach chmur obliczeniowych wymaga dostosowania procesów zarządzania ryzykiem, które zazwyczaj dotyczą lokalnych zasobów fizycznych, systemów i aplikacji. Bardzo istotne jest określenie zakresu odpowiedzialności za realizację poszczególnych usług przetwarzania przy założeniu, że świadczone są one przez zewnętrzne podmioty. Dodatkowo, niezbędne jest spełnienie wymagań bezpieczeństwa i kontroli w stosunku do krytyczności informacji przetwarzanych w modelach chmur obliczeniowych, w sposób opłacalny i wydajny, przy jednoczesnym zapewnieniu bezpieczeństwa realizacji zadań statutowych.

Proces oceny ryzyka przy migracji informacji do przetwarzania w modelach chmur obliczeniowych koncentruje się na ocenie wymagań dla poziomów potencjalnego wpływu na bezpieczeństwo informacji. Potencjalni odbiorcy usług przy wyborze oferty dostawcy usług chmur obliczeniowych kierują się potrzebami operacyjnymi i funkcjonalnymi oraz weryfikują ich zgodność z wymaganiami SCCO na poziomie odpowiadającym klasyfikacji systemu i informacji, które mają być przetwarzane z wykorzystaniem usług chmur obliczeniowych.

Proces zarządzania ryzkiem związanym z przetwarzaniem informacji w modelach chmur obliczeniowych został opisany w poniższym cyklu RMF[8].

[8] Ang. Risk Management Framework



Rysunek 1 Ramy zarządzania ryzykiem zastosowane w ekosystemie chmury - perspektywa Odbiorcy usług w chmurze.

Działania potencjalnych odbiorców usług chmur obliczeniowych związane z zarządzaniem ryzykiem obejmują **następujące kroki**:

1. **Ocena ryzyka** – (analiza środowiska modelu chmur obliczeniowych w celu zidentyfikowania potencjalnych podatności dla bezpieczeństwa informacji)

   Krok 1: Klasyfikacja
   - Klasyfikacja systemu teleinformatycznego i przetwarzanych informacji, przechowywanych i przesyłanych przez ten system na podstawie analizy wpływu systemu na realizację zadań statutowych,
   - Opinia właściwego CSIRT poziomu krajowego, w przypadku planowanego wykorzystania usług publicznych chmur obliczeniowych zgodnie z § 8 uchwały WIIP.

   Krok 2: Selekcja
   - Identyfikacja i wybór możliwości funkcjonalnych dla całego systemu teleinformatycznego, powiązanych z nim podstawowych zabezpieczeń[9] w oparciu o poziom potencjalnego wpływu na bezpieczeństwo informacji, kontrole prywatności i rozszerzone kontrole bezpieczeństwa,
   - Identyfikacja i wybór najlepiej dopasowanego modelu chmury obliczeniowej dla danego systemu teleinformatycznego,

[9] ang. Security Controls

- Ocena dostawców usług chmur obliczeniowych spełniających kryteria zdefiniowane przez potencjalnego odbiorcę usług chmur obliczeniowych (w tym architektura, możliwości funkcjonalne, zarządzanie i monitorowanie usług),
- Wybór dostawców usług chmur obliczeniowych, którzy najlepiej spełniają wymagania funkcjonalne oraz wymagania bezpieczeństwa (najlepiej wybrać dostawcę, który stosuje więcej zabezpieczeń organizacyjnych i technicznych, tak, aby minimalizować liczbę dodatkowych zabezpieczeń, które muszą być stosowane po stronie odbiorcy usług chmur obliczeniowych. Na tym etapie określa się zabezpieczenia, które zostaną wdrożone przez odbiorcę usług chmur obliczeniowych, zabezpieczenia wdrożone przez dostawców usług chmur obliczeniowych w ramach oferowanych usług oraz zabezpieczenia, które należy dostosować (poprzez stosowanie zamiennych zabezpieczeń i wybór określonych parametrów dla tych zabezpieczeń),
- Negocjacja umowy definiującej poziom świadczonych usług chmur obliczeniowych [10] SLA oraz wymagania bezpieczeństwa. Udokumentowanie wszystkich stosowanych zabezpieczeń. Przegląd i zatwierdzenie dokumentu polityki bezpieczeństwa. W przypadku wykorzystania w procesie sytemu ZUCH (usługa świadczona przez Ministra Cyfryzacji) etap negocjacji realizowany jest dla całego katalogu usług PChO, zaś odbiorca otrzymuje standardową umowę zgodną z niniejszymi standardami.

2. **Postępowanie z ryzykiem** (projektowanie, mitygacja, polityki i plany)

Krok 3: Implementacja

- Wdrożenie zabezpieczeń, za które odpowiedzialny jest odbiorca usług chmur obliczeniowych.

Krok 4: Ocena

- Ocena wdrożenia zabezpieczeń przez dostawcę usług chmur obliczeniowych na podstawie przedłożonej dokumentacji,
- Identyfikacja i ocena wszelkich dziedziczonych i zależnych relacji między zabezpieczeniami stosowanymi przez dostawcę i odbiorcę usług chmur obliczeniowych.

Krok 5: Akredytacja

- Decyzja kierownika jednostki organizacyjnej o uruchomieniu systemu teleinformatycznego korzystającego z usług w modelach chmur obliczeniowych, a dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych stosowne dopuszczenie zgodnie z wymaganiami wynikającymi z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

3. **Kontrola ryzyka** (monitorowanie ryzyka, przegląd zdarzeń, korekty w polityce bezpieczeństwa)

[10] ang. Service Level Agreement - SLA

Krok 6: Monitorowanie

- Ciągłe i w czasie rzeczywistym monitorowanie funkcjonowania zabezpieczeń zarządzanych przez odbiorcę usług chmur obliczeniowych,
- Ciągłe i w czasie rzeczywistym monitorowanie funkcjonowania zabezpieczeń zarządzanych przez dostawcę usług chmur obliczeniowych,
- Ponowna ocena i ponowna akredytacja (okresowa lub ciągła) bezpieczeństwa usług świadczonych przez dostawcę usług chmur obliczeniowych.

Opisane powyżej podejście (**schemat sześciu kroków**) umożliwia organizacjom systematyczne stosowanie i monitorowanie zabezpieczeń wspólnych, hybrydowych i specyficznych dla systemów teleinformatycznych oraz formułowanie wymagań bezpieczeństwa uwzględnianych w postępowaniach o zamówienia publiczne na dostawę usług w modelach chmur obliczeniowych.

Odbiorca usług chmur obliczeniowych odpowiada za prowadzenie oceny ryzyka, identyfikację wszystkich wymagań bezpieczeństwa wobec usług w wybranych modelach chmur obliczeniowych oraz weryfikację zabezpieczeń stosowanych przez dostawcę usług chmur obliczeniowych przed zawarciem umowy o świadczenie usług. Weryfikacja zabezpieczeń odbywać się powinna w oparciu o przedłożoną przez dostawcę usług dokumentację.

Dostawcy usług chmur obliczeniowych, którzy w największym stopniu spełniają potrzeby odbiorcy usług chmur obliczeniowych powinni być wybierani z katalogu usług w ramach Systemu Zapewniania Usług Chmurowych – ZUCH lub bezpośrednio w przypadku zamawiania usług poza Wspólną Infrastrukturą Informatyczną Państwa. **Katalog usług ZUCH dostępny jest online po zalogowaniu pod adresem: chmura.gov.pl.**

Umowa o świadczenie usług chmur obliczeniowych **musi zawierać** część szczegółowo określającą rodzaje usług i poziomy usług (SLA), które mają być świadczone, w tym między innymi **czas dostawy, dostępność i parametry wydajnościowe, a także zabezpieczenia na wypadek awarii**.

Odbiorca usług chmur obliczeniowych musi zwrócić szczególną uwagę na postanowienia w umowie odnoszące się do poziomów bezpieczeństwa świadczonych usług, korzystać z opinii zespołów CSIRT i zewnętrznych ekspertów, aby upewnić się, że warunki umowy pozwolą organizacji na realizację zadań statutowych i spełnienie wymagań dotyczących wydajności.

Jednym z wyzwań przy wyborze ofert usług chmur obliczeniowych jest to, że dostawcy usług chmur obliczeniowych mogą oferować domyślną umowę napisaną z perspektywy dostawcy (umowy adhezyjne). Takie domyślne umowy mogą w niewystarczającym stopniu zaspokajać potrzeby odbiorców usług chmur obliczeniowych i choć nie są niedopuszczalne, należy zwrócić na nie szczególną uwagę.

Podsumowując, podjęcie decyzji o migracji systemu teleinformatycznego do modelu chmur obliczeniowych wymaga od organizacji dokładnej identyfikacji własnych wymagań

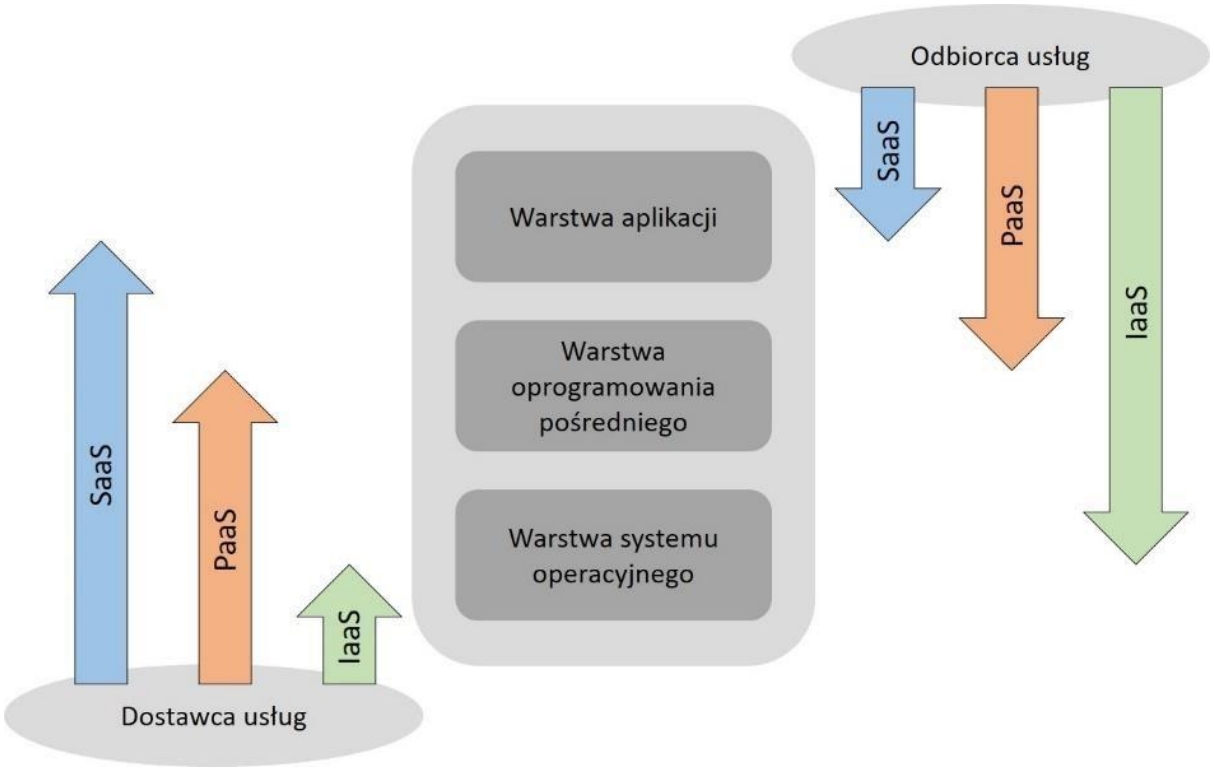
bezpieczeństwa oraz oceny adekwatności zakresu i zabezpieczeń usług oferowanych przez danego dostawcę usług chmur obliczeniowych, wynegocjowania warunków umowy uwzględniających wymagane poziomy bezpieczeństwa usług oraz budowania zaufania z dostawcą usług chmur obliczeniowych przed akredytacją uruchamianych w nich usług przetwarzania informacji.

Szczegółowe szacowanie ryzyka w połączeniu z bezpieczną organizacją ekosystemu chmur obliczeniowych spełniającego wymagania SCCO, wraz z odpowiednimi wskazówkami dotyczącymi negocjowania umów ma wspierać odbiorców usług chmur obliczeniowych w zarządzaniu ryzykiem i podejmowaniu świadomych decyzji w zakresie wykorzystania modeli chmur obliczeniowych, które z założenia powinny zapewniać wyższy poziom bezpieczeństwa od systemów korzystających z lokalnej, dedykowanej infrastruktury teleinformatycznej.

Korzystając z ekosystemu chmur obliczeniowych, odbiorcy usług, jako właściciele informacji powiązanych, pozostają odpowiedzialni za ich zabezpieczenie proporcjonalnie do klasyfikacji informacji. Poziom kontroli i bezpośredniego zarządzania usługami w chmurach obliczeniowych różni się w zależności od wykorzystywanego modelu usług chmur obliczeniowych.

4.1 Współdzielona odpowiedzialność za ochronę zasobów w modelach chmur obliczeniowych

Dostawca i odbiorca usług chmur obliczeniowych współdzielą kontrolę nad zasobami środowiska. Jak pokazano na rysunku 2, różne modele usług w chmurach obliczeniowych wpływają na kontrolę organizacji nad zasobami obliczeniowymi, a tym samym na to, jakie działania możliwe są w środowisku chmury obliczeniowej. Rysunek pokazuje te różnice za pomocą klasycznej notacji stosu oprogramowania złożonej z warstw aplikacji, oprogramowania pośredniego i systemu operacyjnego. Analiza kontroli nad stosem aplikacji pomaga zrozumieć obowiązki stron zaangażowanych w zarządzanie aplikacją w chmurze obliczeniowej.



Rysunek 2: Zakres podziału odpowiedzialności pomiędzy dostawcą a odbiorcą usług chmur obliczeniowych (Na podstawie NIST SP 500-292)

Warstwa aplikacji obejmuje aplikacje skierowane do użytkowników końcowych lub programów korzystających z usług chmur obliczeniowych. Aplikacje są:

- używane przez odbiorców usług typu SaaS[11] („oprogramowanie jako usługa")
- instalowane/zarządzane/obsługiwane przez odbiorców usług typu PaaS [12] („platforma aplikacyjna jako usługa"), odbiorców usług typu IaaS[13] („infrastruktura jako usługa") oraz dostawców usług typu SaaS.

Warstwa oprogramowania pośredniego zapewnia bloki konstrukcyjne oprogramowania (np. biblioteki, bazę danych i maszynę wirtualną) do wytwarzania oprogramowania w środowisku chmury obliczeniowej. Oprogramowanie pośrednie jest:

- używane przez odbiorców usług typu PaaS,
- instalowane/zarządzane/obsługiwane przez odbiorców usług typu IaaS lub dostawców usług typu PaaS i pozostaje niewidoczna dla użytkownika końcowego usług typu SaaS.

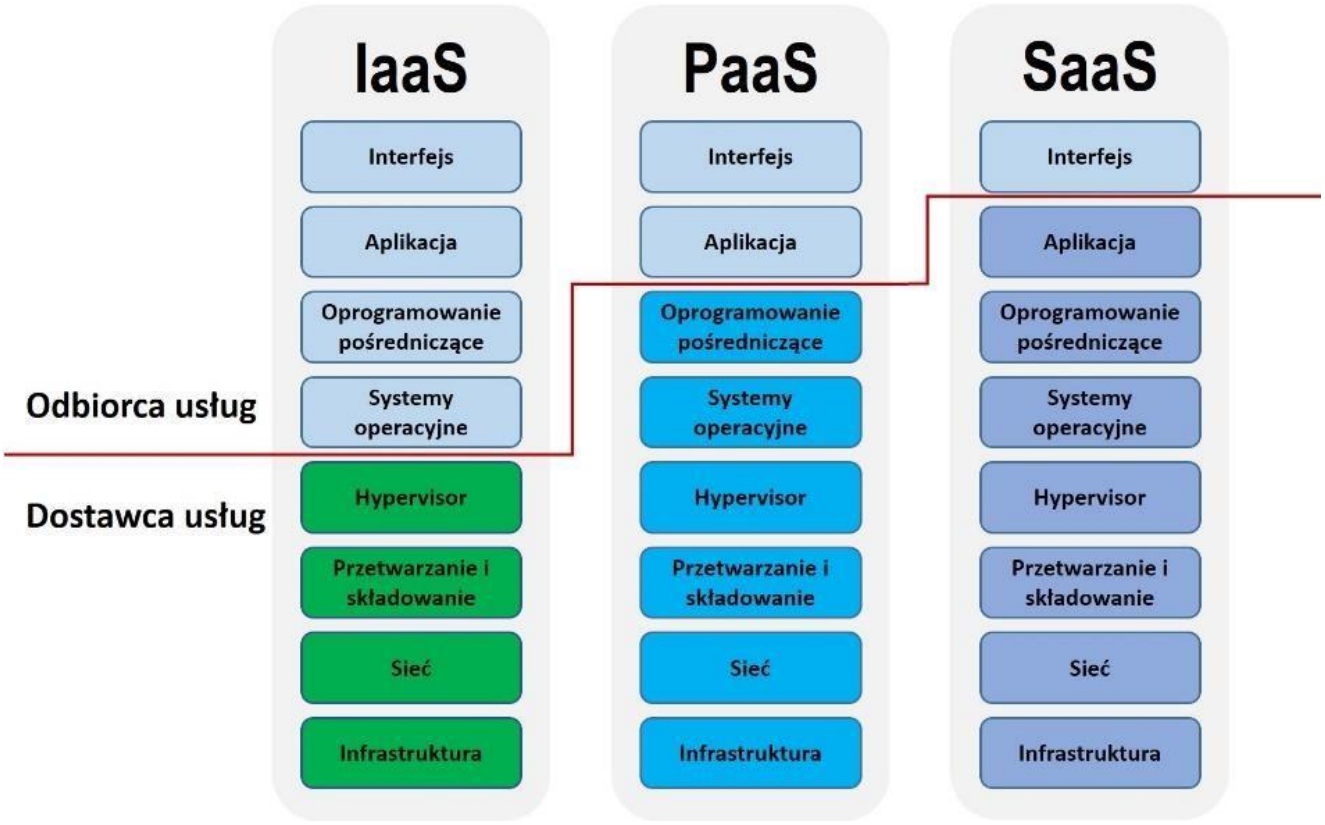
Warstwa systemu operacyjnego obejmuje system operacyjny oraz sterowniki i jest ukryta przed odbiorcami usług typu SaaS i PaaS. Usługa chmur obliczeniowych typu IaaS umożliwia uruchamianie wirtualizacji jednego lub wielu systemów operacyjnych na jednym hoście fizycznym. Zasadniczo odbiorcy usług chmur obliczeniowych mają dużą swobodę wyboru,

[11] ang. Software as a Service - SaaS
[12] ang. Platform as a Service - PaaS
[13] ang. Infrastructure as a Service - IaaS

który system operacyjny ma być hostowany spośród wszystkich systemów operacyjnych, które obsługiwane są przez danego dostawcę usług chmur obliczeniowych. Odbiorcy usług typu IaaS odpowiadają za utrzymanie, administrowanie i bezpieczeństwo systemu operacyjnego, a dostawca usługi typu IaaS odpowiada za utrzymanie, administrowanie i bezpieczeństwo systemu operacyjnego środowiska hosta.

Modele usługowe chmur obliczeniowych definiowane są w ramach stosu SPI – Software, Platform, Infrastructure as a Service. Pozwala on w uproszczony sposób zilustrować, jakie elementy usługi są dostarczane przez dostawcę, a za jakie elementy danego modelu usługowego odpowiada odbiorca usług chmur obliczeniowych. Ma to istotne znaczenie w zrozumieniu, jakie ryzyka są związane z poszczególnymi modelami oraz pomaga określić, kto jest odpowiedzialny za minimalizację tych ryzyk i zastosowanie odpowiednich zabezpieczeń.

Rysunek 3 przedstawia typowy układ stosu SPI.



Rysunek 3: Stos SPI

Odbiorca usług chmur obliczeniowych musi rozumieć zakres swojej odpowiedzialności przy korzystaniu z usług i uwzględnić to w ocenie ryzyka i zakresie działań zabezpieczających.

4.2 Wymagania bezpieczeństwa dla usług w publicznej i rządowej chmurze obliczeniowej

Bazując na definicji poziomów wymagań bezpieczeństwa SCCO przedstawionych w Rozdziale 3.2 stosowane są następujące zasady oceny usług świadczonych przez dostawców usług publicznych chmur obliczeniowych:

Poziom SCCO1: informacje na tym poziomie mogą być hostowane przez dostawcę usług publicznych chmur obliczeniowych. Odbiorca usług publicznych chmur obliczeniowych na poziomie SCCO1 odpowiada za sprawdzenie czy katalog usług danego dostawcy usług publicznych chmur obliczeniowych spełnia wymagania **podstawowych zabezpieczeń** dla **niskiego lub umiarkowanego poziomu potencjalnego wpływu na bezpieczeństwo** zgodnie z Załącznikiem 5 do SCCO – bazującym na pełnym wykazie zabezpieczeń na podstawie NIST SP 800-53.

***Poziom SCCO2*:** informacje na tym poziomie mogą być hostowane przez dostawcę usług publicznych chmur obliczeniowych, który deklaruje zgodność stosowanych **podstawowych zabezpieczeń** z wymaganiami na **umiarkowanym lub wysokim poziomie potencjalnego wpływu na bezpieczeństwo** zgodnie z Załącznikiem 5 do SCCO, a dodatkowo – o ile to wymagane – zgodność stosowanych zabezpieczeń rozszerzonych.

Deklaracja zgodności, dostarczana przez dostawcę usług chmurowych, powinna zawierać szczegółowe zestawienie stosowanych zabezpieczeń z ich odniesieniem do macierzy zabezpieczeń SCCO.

Pozytywna weryfikacja deklaracji zgodności przez Ministerstwo Cyfryzacji będzie podstawą do umieszczenia oferty usług chmur obliczeniowych danego dostawcy w katalogu usług publicznych chmur obliczeniowych PChO, dostępnym dla jednostek administracji publicznej.

W niektórych przypadkach konieczne będzie skorzystanie z usług RChO z uwagi na kategorię przetwarzanych danych.

Poziom SCCO3: informacje na tym poziomie mogą być hostowane przez dostawcę usług publicznych chmur obliczeniowych, który deklaruje zgodność stosowanych podstawowych zabezpieczeń z wymaganiami na wysokim poziomie potencjalnego wpływu na bezpieczeństwo zgodnie z Załącznikiem 5 do SCCO, zgodność stosowanych zabezpieczeń rozszerzonych oraz spełnione zostaną wymagania dla ochrony informacji niejawnych właściwe do klauzuli przetwarzanych informacji niejawnych.

Należy ponownie wskazać na zastrzeżenia co do alokacji CPD wskazane w tabeli dotyczącej kategorii informacji.

Rządowa Chmura Obliczeniowa: Usługi ujęte w **katalogu usług RChO** są dostarczane i obsługiwane przez operatora Rządowej Chmury Obliczeniowej. Usługi RChO są objęte takim samym zakresem podstawowych zabezpieczeń jak usługi dostawców publicznych chmur

obliczeniowych, z dodatkowymi środkami ochrony wymaganymi na poziomie SCCO2 lub 3, dotyczącymi w szczególności:

- zabezpieczeń organizacyjnych i technicznych dla Centrów Przetwarzania Danych przyłączonych do RChO,
- usług Rządowego Klastra Bezpieczeństwa,
- poświadczeń bezpieczeństwa dla personelu odpowiedzialnego za usługi świadczone w RChO.

5. Wymagania bezpieczeństwa

W tym rozdziale wskazane zostały wymagania bezpieczeństwa dotyczące korzystania z usług chmur obliczeniowych przez jednostki administracji publicznej.

5.1 Wymagania bezpieczeństwa przetwarzania informacji w chmurach obliczeniowych

Wymaga się, aby wszystkie systemy teleinformatyczne oraz informacje z jednostek administracji publicznej, które mają być przetwarzane z wykorzystaniem usług w modelu chmur obliczeniowych:

- zostały skategoryzowane zgodnie z załącznikiem 2 do Uchwały WIIP[14],
- sklasyfikowane pod kątem poziomu wymagań bezpieczeństwa SCCO, zgodnie z rozdziałem 3.2.

5.2 Jurysdykcja – uregulowania unijne dotyczące dostawców usług cyfrowych

Zgodnie z *Artykułem 26* dyrektywy UE 2022/2555[15]

1. Dostawca usług chmurowych podlega jurysdykcji państwa członkowskiego UE, w którym ma główne miejsce prowadzenia działalności w Unii. Dostawca usług chmurowych ma swoje główne miejsce prowadzenia działalności w Unii w tym państwie członkowskim, w którym przeważnie podejmuje decyzje związane ze środkami zarządzania ryzykiem w cyberbezpieczeństwie. Jeżeli nie można ustalić takiego państwa członkowskiego lub jeżeli takich decyzji nie podejmuje się w Unii, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym prowadzone są działania w zakresie cyberbezpieczeństwa. Jeżeli nie można ustalić takiego państwa członkowskiego, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie

[14] Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (Monitor Polski z dnia 24 września 2019 r. poz. 862).

[15] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333/80 z 27.12.2022).

członkowskim, w którym dany dostawca usług chmurowych ma miejsce prowadzenia działalności o największej liczbie pracowników w Unii.

2. Jeżeli dostawca usług chmurowych nie ma miejsca prowadzenia działalności w Unii, ale oferuje usługi w Unii, wyznacza przedstawiciela w Unii. Przedstawiciel musi mieć miejsce prowadzenia działalności w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że taki podmiot podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel ma miejsce prowadzenia działalności.

Zgodnie z załącznikiem 2 do Uchwały WIIP informacje administracji publicznej mogą być przetwarzane z wykorzystaniem usług w publicznych chmurach obliczeniowych znajdujących się w jurysdykcji polskiej lub w jurysdykcji państwa członkowskiego UE lub EOG. SCCO na odpowiednich poziomach doprecyzowuje, że państwo EOG musi stosować prawo UE.

Dostawca usług przetwarzania w publicznych chmurach obliczeniowych umieszczanych przez Ministerstwo Cyfryzacji w katalogu usług PChO zobowiązany jest do przedstawienia listy wszystkich fizycznych lokalizacji centrów przetwarzania danych, w których dane mogą być przechowywane i przetwarzane. Dostawca usług przetwarzania w publicznych chmurach obliczeniowych, który nie został umieszczony w katalogu usług PChO powinien przed zawarciem umowy o świadczenie usług, na żądanie podmiotu administracji, przedstawić listę wszystkich fizycznych lokalizacji centrów przetwarzania danych, w których dane mogą być przechowywane i przetwarzane.
Odnośnik do zabezpieczeń: SA-9 (Załącznik 5)

5.2.1 Wykorzystanie danych administracji publicznej przez dostawców usług publicznych chmur obliczeniowych

Wszystkie informacje/dane umieszczone lub utworzone przez administrację publiczną w chmurze dostawcy usług publicznych chmur obliczeniowych są własnością właściciela informacji, chyba, że została zawarta umowa z dostawcą usług, która stanowi inaczej. Dostawca usług publicznych chmur obliczeniowych nie ma żadnych praw do informacji / danych administracji publicznej. Informacje / dane obejmują także dzienniki i dane monitorowania utworzone przez aplikacje i systemy odbiorcy usług publicznych chmur obliczeniowych.

Dostawca usług publicznych chmur obliczeniowych **nie może** wykorzystywać informacji / danych odbiorców usług w żaden inny sposób aniżeli określony w umowie o świadczenie usług.

Dostawca usług publicznych chmur obliczeniowych zachowuje własność wszystkich dzienników i danych monitorowania związanych z wykorzystaniem i zarządzaniem świadczonymi usługami przetwarzania w publicznej chmurze obliczeniowej. Zalecane jest jednak, aby w umowie o świadczenie usług chmurowych uregulować, że dostawca usług publicznych chmur obliczeniowych niezwłocznie, na każde żądanie odbiorcy usług, przekazuje zawartość wszystkich dzienników i danych monitorowania związanych z wykorzystaniem i zarządzaniem świadczonymi usługami przetwarzania w publicznej chmurze obliczeniowej związanych z odbiorcą usług. Takie postanowienie przyczyni się do realizacji założonego celu

jakim jest zapewnienie większej kontroli odbiorcy usługi nad procesem przetwarzania danych w chmurze obliczeniowej poprzez dostarczenie mu szczegółowych informacji.

Dostawca usług publicznych chmur obliczeniowych **nie może** ujawniać danych odbiorców usług korzystających z jego oferty usług chmur obliczeniowych:

- organom państw, w których są przetwarzane dane tych odbiorców usług,
- organom państw sprawujących jurysdykcję nad dostawcą usług – o ile nie wynika to wprost z umowy zawartej pomiędzy odbiorcą i dostawcą usług.

Dostawca usług publicznych chmur obliczeniowych zobowiązany jest do niezwłocznego poinformowania odbiorcy usług o obowiązywaniu lub wprowadzeniu prawa uniemożliwiającego spełnienie powyższych warunków.
Odnośnik do zabezpieczeń: AC-23 (Załącznik 5)

5.3 Migracja i postępowanie z danymi po zaprzestaniu przetwarzania z wykorzystaniem usług w chmurze obliczeniowej

Niszczenie danych to zestaw działań, które mają miejsce, gdy jednostka administracji publicznej zaprzestanie korzystania z usług chmury obliczeniowej danego dostawcy. Proces przeniesienia jest wymagany, gdy Właściciel systemu migruje dane do innego dostawcy usług chmur obliczeniowych, wygasa umowa z dostawcą lub dostawca usług przestaje świadczyć usługi chmur obliczeniowych. Proces wyjścia z chmury jest podzielony na dwa etapy:

- pobieranie / migracja danych
- usuwanie lub zniszczenie danych.

Odbiorcy usług w chmurach obliczeniowych muszą przygotować się na ewentualne wycofanie usługi z oferty, a dostawcy usług zobowiązani są do niezwłocznego powiadomienia odbiorców usług o planowanym zaprzestaniu świadczenia usług chmur obliczeniowych.

Komercyjni dostawcy usług w chmurach obliczeniowych zobowiązani są do stosowania technologii pozwalających na łatwą migrację danych do infrastruktury własnej odbiorcy usługi lub infrastruktury innego dostawcy usług chmurowych. Ma to na celu zapewnienie konkurencyjności, odpowiedniego poziomu bezpieczeństwa, w szczególności poprzez wyeliminowanie zagrożenia tzw. „vendor lock-in" czyli uzależnienia odbiorcy usługi od jednego dostawcy. Komercyjny dostawca usługi powinien zatem stosować odpowiedniego rodzaju technologie umożliwiające szybką i nisko kosztową zmianę dostawcy usługi przetwarzania w chmurze obliczeniowej.

Umowa o świadczenie usług chmur obliczeniowych musi zawierać część określającą warunki zakończenia korzystania z usług chmury obliczeniowej, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych danych.

5.4 Wycofanie z użycia, ponowne użycie i niszczenie nośników pamięci i sprzętu

Dostawca usług w chmurze obliczeniowej zobowiązany jest do upewnienia się, że nie pozostały żadne dane odbiorców usług na urządzeniach pamięci, które zostały wycofane z eksploatacji i zniszczone, ponownie wykorzystane w środowisku nieobjętym umową między dostawcą usług a odbiorcą usług lub przekazane osobom trzecim; zgodnie z wymaganiami zabezpieczeń MP-6 (Załącznik 5).

5.5 Kryptograficzna ochrona informacji

5.5.1 Polityka dotycząca stosowania procedur szyfrowania i zarządzania kluczami

Kryptograficzna ochrona informacji przetwarzanych z wykorzystaniem usług chmur obliczeniowych powinna uwzględniać następujące zasady i instrukcje stosowania organizacyjnych i technicznych zabezpieczeń:

- Korzystanie z silnych algorytmów szyfrowania (np. AES) i stosowanie najnowszych bezpiecznych protokołów sieciowych (np. TLS, IPsec, SSH):
  - BSI TR-02102-2 Mechanizmy kryptograficzne: zalecenia i długości klucza część 2 - Korzystanie z Transport Layer Security (TLS)
  - BSI TR-02102-3 Mechanizmy kryptograficzne: zalecenia i długości klucza Część 3 - Korzystanie z zabezpieczeń protokołu internetowego (IPSec) i Internet Key Exchange (IKEv2)
  - BSI TR-02102-4 Mechanizmy kryptograficzne: zalecenia i długości klucza Część 4 - Korzystanie z bezpiecznej powłoki (SSH)

5.5.2 Szyfrowanie transmisji danych

Transmisja danych przetwarzanych w modelach chmur obliczeniowych powinna podlegać ochronie kryptograficznej polegającej na szyfrowaniu. Wymagania dotyczące mechanizmów kryptograficznych (algorytmów i długości kluczy) znajdują się w aktualizowanym okresowo dokumencie BSI TR-02102 Cryptographic Mechanisms[16].

Silne szyfrowanie transmisji realizowane jest obecnie z wykorzystaniem protokołu TLS 1.3, a jeśli nie jest dostępny to TLS 1.2.w połączeniu z Perfect Forward Secrecy.

5.5.3 Szyfrowanie wrażliwych danych na pamięci masowej

W celu przetwarzania i przechowywania wrażliwych informacji odbiorca usług chmur obliczeniowych powinien ustanowić procedury i wybrać techniczne zabezpieczenia do ich szyfrowania. Wyjątki dotyczą informacji, które nie mogą być zaszyfrowane w celu świadczenia usługi w chmurze obliczeniowej ze względów funkcjonalnych.

[16] https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/index_htm.html

Klucze prywatne używane do szyfrowania powinny być znane tylko odbiorcy usług chmur obliczeniowych. Wyjątki (np. użycie klucza głównego przez dostawcę usług chmury obliczeniowej) opierają się na kontrolowanej procedurze i muszą być uzgodnione z odbiorcą usług chmury obliczeniowej.

5.5.4 Bezpieczne zarządzanie kluczami

Procedury i zabezpieczenia techniczne dla bezpiecznego zarządzania kluczami obejmują, co najmniej, następujące aspekty:

- generowanie kluczy dla różnych systemów kryptograficznych i aplikacji
- wydawanie i uzyskiwanie certyfikatów klucza publicznego
- obsługa i aktywacja kluczy dla odbiorców usług chmur obliczeniowych
- bezpieczne przechowywanie kluczy kryptograficznych
- wymiana lub aktualizacja kluczy kryptograficznych, w tym zasad określających, w jakich warunkach i w jaki sposób wymiana lub aktualizacja ma być realizowana
- wycofanie i usunięcie kluczy, na przykład w przypadku naruszenia bezpieczeństwa lub zmiany personelu
- przechowywanie kluczy odbiorców usług chmury publicznej poza środowiskiem dostawcy usług (np. u zaufanej strony trzeciej).

5.5.5 Szyfrowanie danych w chmurach obliczeniowych

Odbiorcy usług w chmurach obliczeniowych muszą mieć możliwość szyfrowania informacji / danych podczas ich przechowywania i transmisji z zapewnieniem wyłącznej kontroli odbiorcy usług nad procesami generowania i zarządzania kluczami.

Dostawcy usług w chmurach obliczeniowych mogą oferować dedykowane sprzętowe kryptograficzne moduły bezpieczeństwa[17] lub oferować generowanie i zarządzanie kluczami kryptograficznymi, jako jedną z usług bezpieczeństwa. Dane na poziomie SCCO 3 i SCCO 4 powinny być obligatoryjnie szyfrowane przy użyciu sprzętowych kryptograficznych modułów bezpieczeństwa.

Szyfrowanie informacji / danych przechowywanych w środowisku chmury obliczeniowej przy użyciu kluczy kontrolowanych i zarządzanych przez odbiorcę usługi daje następujące korzyści:

- chroni integralność publicznie udostępnianych informacji i zawartość stron internetowych na poziomie SCCO1, gdzie zachowanie poufności nie jest głównym wymaganiem,
- chroni poufność i integralność na poziomie SCCO1, SCCO2 i SCCO3, dodatkowo:
  - ogranicza zagrożenia wewnętrzne związane z uzyskaniem nieuprawnionego dostępu przez pracowników dostawcy usług w chmurze obliczeniowej
  - ogranicza zagrożenia zewnętrzne związane z uzyskaniem nieuprawnionego dostępu przez zewnętrznych atakujących

[17] ang. Hardware Security Module - HSM

– umożliwia wysoce niezawodne zabezpieczenia dostępu do informacji przy konieczności migracji i/lub zakończenia korzystania z usług przetwarzania w chmurze obliczeniowej danego dostawcy bez konieczności udziału lub współpracy z tym dostawcą.

5.5.6 Kasowanie kryptograficzne

Kasowanie kryptograficzne jest techniką kasowania, która może być stosowana w niektórych sytuacjach, gdy dane przechowywane na nośniku są zaszyfrowane. W tym przypadku kasowanie nośników odbywa się poprzez kasowanie kluczy kryptograficznych używanych do szyfrowania danych, w przeciwieństwie do kasowania pamięci na nośnikach zawierających same zaszyfrowane dane. *[NIST SP 800-88]*

Szyfrowanie przechowywanych informacji, w połączeniu z wyłączną kontrolą odbiorcy usług w chmurze obliczeniowej nad zarządzaniem kluczami kryptograficznymi, zapewnia możliwość kryptograficznego usuwania danych bez pomocy i współpracy z dostawcą usług.

5.5.7 Szczególne wymagania kryptograficznej ochrony informacji poziomu SCCO 3 i SCCO 4

Przepisy prawa powszechnie obowiązującego, w szczególności ustawa o ochronie informacji niejawnych i akty wykonawcze, takie jak Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego [18] stanowią o bezpieczeństwie systemów teleinformatycznych podlegających akredytacji bezpieczeństwa teleinformatycznego z uwagi na to, że mają być w nich przetwarzane informacje niejawne.

Informacje niejawne – w różnym zakresie i w różnym modelu, na co wskazują poziomy SCCO 3 i SCCO 4 – mogą być przetwarzane w chmurze obliczeniowej. W związku z charakterem tych informacji zastosowanie do nich muszą mieć szczególne wymagania z zakresu bezpieczeństwa. Oznacza to, że w zakresie w jakim wymagania kryptograficznej ochrony informacji wskazane we wcześniejszych sekcjach nie odpowiadają poziomowi wymagań określonych w aktach prawa powszechnie obowiązującego, zastosowanie powinny znaleźć wymagania wyższego poziomu, określone w tych aktach. W szczególności należy brać pod uwagę §10 ust. 2 i 3 Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego oraz art. 50 ustawy o ochronie informacji niejawnych.

5.6 Kopia zapasowa

Dostawcy usług w chmurach obliczeniowych wykorzystywanych przez administrację publiczną są odpowiedzialni za tworzenie kopii zapasowych danych zgodnie z zabezpieczeniem CP-9

[18] Dz.U.2011.159.948.

(Załącznik 5), w sposób umożliwiający ich odtworzenie przez odbiorcę usługi. Odbiorcy usług w chmurach obliczeniowych są również odpowiedzialni za zapewnienie kopii zapasowej ich danych zgodnie z zabezpieczeniem CP-9.

Dodatkowe kopie zapasowe przechowywane u więcej niż jednego dostawcy usług w chmurach obliczeniowych zmniejszają ryzyko utraty / uszkodzenia informacji / danych w przypadku zaprzestania działalności lub katastrofalnego zdarzenia, które wpływa na całą infrastrukturę dostawcy usług. Decyzja dotycząca liczby dodatkowych kopii zapasowych i miejsca ich przechowywania powinna być podejmowana na podstawie analizy ryzyka w ramach planowania awaryjnego wymaganego przez zabezpieczeniem CP-2.

UWAGA: W przypadku kopii zapasowych w usługach typu IaaS / PaaS kopie zapasowe obejmują konfiguracje maszyn wirtualnych lub obrazy w pełni skonfigurowanych maszyn wirtualnych, w tym ich wirtualnych dysków twardych, dzięki czemu odtworzenie bazy obliczeniowej i informacji jest łatwiejsze. Zabezpieczenia: CP-2, CP-9.

6. Obsługa incydentów przy korzystaniu z usług w modelach chmur obliczeniowych

Wymagania dotyczące obsługi incydentów zostały zawarte w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [uKSC].

Dostawcy usług chmurowych stosują, w ramach systemu zarządzania bezpieczeństwem informacji, środki zarządzania ryzykiem określone w rozporządzeniu wykonawczym 2024/2690. Środki te zapewniają cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają w szczególności:

1) bezpieczeństwo systemów informacyjnych i obiektów;
2) postępowanie w przypadku obsługi incydentu;
3) zarządzanie ciągłością działania dostawcy;
4) monitorowanie, audyt i testowanie;
5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2024/2690.

Podmioty administracji publicznej będące odbiorcami usług w chmurach obliczeniowych podlegają obowiązkom określonym w rozdziale 5 uKSC (art. 21-25) oraz są zobowiązane do spełnienia wymagań dotyczących systemu zarządzania bezpieczeństwem informacji, o których mowa w §19 rozporządzenia KRI[19]. Każdy podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego:

1) zapewnia zarządzanie incydentem w podmiocie publicznym;

[19] 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.

2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;
5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

Należy zauważyć, że dyrektywa 2022/2555 określa nowe wymagania w zakresie cyberbezpieczeństwa i na nowo określa zadania i obowiązki dostawców usług chmurowych i podmiotów administracji publicznej w tym zakresie. Po wdrożeniu dyrektywy 2022/2555 do porządku krajowego dostawcy usług chmurowych i podmioty administracji publicznej powinny brać pod uwagę nowe przepisy świadcząc bądź korzystając z usług przetwarzania w chmurze obliczeniowej. Z przepisów tych wynikają bowiem nowe wymagania, obowiązki dla podmiotów ważnych i kluczowych, w tym podmiotów administracji publicznej oraz wprowadzane są nowe środki nadzoru.

7. Wymagania dla CPD zarządzanych przez podmioty administracji rządowej

Najważniejsze wymagania dla CPD zarządzanych przez podmioty administracji rządowej określone zostały w załączniku nr 1 do uchwały WIIP i §19 rozporządzenia KRI.

Wskazać również należy, że dyrektywa 2022/2555 i rozporządzenie wykonawcze 2024/2690 nakładają obowiązki na dostawców usług centrum przetwarzania danych i kształtują w związku z tym wymagania dla CPD. Na posiadaczach CPD spoczywa obowiązek dokonania analizy ww. aktów, a następnie aktu prawnego wdrażającego dyrektywę 2022/2555 w celu weryfikacji, czy wskazane tam obowiązki i wymagania techniczne odnoszą się do tego posiadacza CPD. W przypadku pozytywnej samoidentyfikacji posiadacze CPD obowiązani są do wdrożenia niezbędnych środków zapewniających prawidłową realizację obowiązków wynikających z dyrektywy 2022/2555 i odpowiedni poziom bezpieczeństwa. Zgodnie z dyrektywą 2022/2555 usługa centrum przetwarzania danych powinna obejmować świadczenie usługi, w skład której wchodzą struktury lub grupy struktur służące scentralizowanemu hostingowi, wzajemnym połączeniom i eksploatacji sprzętu informatycznego i sieciowego służącego do przechowywania, przetwarzania i transportu danych wraz z całością obiektów i infrastruktury zapewniających dystrybucję energii elektrycznej i kontrolę środowiskową.

Podkreślić należy, że dyrektywa 2022/2555 jest wdrażana do porządku krajowego projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC 32). Ustawa wdrażająca może w odmienny sposób uregulować kwestie wynikające z dyrektywy, korzystając z prawa do harmonizacji minimalnej. Wdrożone środki powinny być jednak zgodne z celem aktu unijnego. Posiadacz CPD powinien przeanalizować swoją sytuację w szczególności pod kątem tego, czy usługi będzie świadczył na zewnątrz, a jeśli tak, spełnić wymagania określone w dyrektywie 2022/2555 i rozporządzeniu wykonawczym 2024/2690.

Załącznik 1 – Wykaz przepisów i norm związanych bezpieczeństwem przetwarzaniem informacji w modelach chmur obliczeniowych

[1] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2024 r. poz. 1557).
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781).
[3] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2024 r. poz. 34).
[4] Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U. z 2024 r. poz. 1221).
[5] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077).
[6] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2024 r. poz. 632).
[7] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r. poz. 122).
[8] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2025 r. poz. 24).
[9] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902).
[10] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2024 r. poz. 1513).
[11] Ustawa z dnia 5 września 2016 o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2024 r. poz. 422).
[12] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206)
[13] 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 dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773).
[14] Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (Monitor Polski z 2021 r. poz. 1006).
[15] Uchwała nr 42 Rady Ministrów z dnia 16 kwietnia 2020 r. zmieniająca uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (Monitor Polski z 2020 r. poz. 403).
[16] Uchwała nr 127 Rady Ministrów z dnia 23 października 2024 r. zmieniająca uchwałę w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa" (Monitor Polski z 2024 r. poz. 908).
[17] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (Monitor Polski z 2019 r. poz. 1037).
[18] Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. z 2018 r. poz. 2180).
[19] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948.)
[20] Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz. U. z 2020 r. poz. 399).
[21] Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie

bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania (Dz. U. UE L z 18.10.2024)

[22] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (Dz.U. UE L 257/73 z 28.08.2014).

[23] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie (Dz.U. UE L 151/15 z 07.06.2019).

[24] Rozporządzenie 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 (RODO) (Dz. U. UE L 119/1 z 2016 r.).

[25] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/1535 z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241/1 z 17.9.2015).

[26] Dyrektywa Parlamentu Europejskiegoi Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

[27] NIST-US Government Cloud Computing Technology Roadmap Volume II [500-293]

[28] NIST-US Government Cloud Computing Technology Roadmap Volume I [500-293]

[29] NIST-Trusted Cloud Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (laaS) [1800-19B]

[30] NIST-Trusted Cloud Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (laaS) [180019A]

[31] NIST-Technical Guide to Information Security Tested and Assessment [800-115]

[32] NIST-Security_Reference_Architecture_2013.05.15_v1.0 [500-299]

[33] NIST-Security and Privacy Controls for Federal Information Systems and Organizations [800-53]

[34] NIST-Risk Management Framework for Information Systems and Organizations [800-37]

[35] NIST-Recommendation for the Triple Data Encryption Algorithm (TDEA) [800-67]

[36] NIST-Mobile Device Security Cloud and Hybrid Builds Executive Summary How-to Guides [1800-4c]

[37] NIST-Mobile Device Security Cloud and Hybrid Builds Executive Summary [1800-4a]

[38] NIST-Mobile Device Security Cloud and Hybrid Builds Approach, Architecture, and Security Characteristics [1800-4b]

[39] NIST-Mobile Device Security Cloud and Hybrid Builds [1800-4]

[40] NIST-Managing Information Security Risk [800-39]

[41] NIST-Identity and Access Management (IAM) [1800-2]

[42] NIST-Guidelines on Security and Privacy i Public Cloud Computing [800-144]

[43] NIST-Guidelines for Media Sanitization [800-88]

[44] NIST-Guideline for Using Cryptographic Standards in the Federal Government-Directives, Mandates and Policies [800-175B]

[45] NIST-Guideline for Using Cryptographic Standards in the Federal Government [800-175B]

[46] NIST-Guide to Storage Encryption Technologies for End User Devices [800-111]

[47] NIST-Guide to SSL VPNs [800-113]

[48] NIST-Guide to Selecting Information Technology Security Products [800-36]

[49] NIST-Guide to IPsec VPNs [800-77]

[50] NIST-Guide for Security-Focused Configuration Management of Information Systems [SP 800-128]

[51] NIST-Guide for Mapping Types of Information and Information Systems to Security Categories [800-60]

[52] NIST-Definition of Cloud Computing [800-145]

[53] NIST-Cybersecurity Framework Manufacturing Profile [NISTIR 8183]

[54] NIST-Cybersecurity Framework [CSF

[55] NIST-Contingency Planning Guide for Federal Information Systems [800-34]

[56] NIST-Cloud Computing Synopsis and Recommendations [800-146]

[57] NIST-Cloud Computing Standards Roadmap [500-291]

[58] NIST-Cloud Computing Service Metrics Description [500-307]

[59] NIST-Cloud Computing Reference Architecture [500-292]

[60] NIST-Assessing Security and Privacy Controls in Federal Information Systems and Organizations [800-53A]
[61] NIST-ABAC How-to Guides [1800-3C]
[62] NIST-ABAC Executive Summary [1800-3A]
[63] PN-EN ISO/IEC 15408-1:2024-05 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Kryteria oceny zabezpieczeń informatycznych -- Część 1: Wprowadzenie i model ogólny
[64] PN-EN ISO/IEC 18045: 2024-04 Technika informatyczna, cyberbezpieczeństwo i ochrona prywatności - Kryteria oceny zabezpieczeń informatycznych- Metodyka oceny zabezpieczeń informatycznych
[65] PN-EN ISO 22301:2020-04 Bezpieczeństwo i odporność -- Systemy zarządzania ciągłością działania -- Wymagania
[66] PN-EN ISO/IEC 27001:2023-08 - Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - - Systemy zarządzania bezpieczeństwem informacji – Wymagania.
[67] PN-EN ISO/IEC 27002: 2023-01 Bezpieczeństwo informacji, cyberbezpieczeństwoiochrona prywatności - Zabezpieczanie informacji.
[68] PN-ISO/IEC 27004: 2017 - Zarządzanie bezpieczeństwem – Monitorowanie, pomiary, analiza i ocena.
[69] ISO/IEC 27005: 2022 Information security, cybersecurity and privacy protection — Guidanceon managing informationsecurity risks.
[70] PN-EN ISO/IEC 27017:2021-07 - Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze.
[71] PN-EN ISO/IEC 27018:2020-11 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady ochrony informacji o identyfikowalnych osobach (PII) w chmurach publicznych działających jako przetwarzający PII
[72] PN-EN 50600 - seria norm dot. wyposażenia i infrastruktury centrów przetwarzania danych.
[73] NCI – DCIS Cube Architecting Initiative.
[74] CSA – Cloud Controls Matrix (CSA CCM).

Załącznik 2 – Słownik pojęć

Nazwa	Skrót	Opis
Centrum Przetwarzania Danych	**CPD**	**ang. Data Center**. Serwerownia w zasobach administracji rządowej lub obiekt budowlany wykorzystywany jako lokalizacja dla infrastruktury teleinformatycznej i związanych z nią elementów, np.: systemów telekomunikacyjnych, zasobów przetwarzania wraz z nadmiarowymi źródłami zasilania, dodatkowymi sieciami teletransmisji, środkami kontroli środowiska (np. klimatyzacją, systemami gaśniczymi), urządzeniami i systemami bezpieczeństwa oraz ochroną fizyczną obiektu.
Chmura hybrydowa		**ang. hybrid cloud**. Model wdrażania chmury obliczeniowej, w którym infrastruktura składa się z dwóch lub więcej odrębnych infrastruktur teleinformatycznych dostarczanych z chmury obliczeniowej (prywatnej, wspólnotowej lub publicznej), które pozostają odrębnymi jednostkami powiązanymi ze sobą znormalizowaną lub zastrzeżoną technologią, umożliwiającą przenoszenie danych i aplikacji między chmurami obliczeniowymi (np. w celu równoważenia obciążenia);

Chmura Obliczeniowa/ Przetwarzanie w chmurze obliczeniowej		**ang**. **cloud computing**. Model przetwarzania umożliwiający powszechny i wygodny dostęp za pośrednictwem sieci do wspólnej puli konfigurowalnych zasobów przetwarzania (np. sieci, serwerów, pamięci masowych, aplikacji i usług), które mogą być szybko udostępniane przy minimalnym wysiłku ze strony zespołów zarządzania lub dostawcy usług. Chmura obliczeniowa poprzez **katalog usług** dostarcza usługi w modelu chmurowym. Model chmurowy (model chmury obliczeniowej) składa się z pięciu zasadniczych cech (samoobsługi na żądanie, szerokiego dostępu do sieci, dynamicznego gromadzenia zasobów, szybkiego i elastycznego przydzielania i zwalniania zasobów, pomiarów i optymalizacji usług); trzech modeli usług (**SaaS**, **PaaS**, **IaaS**); oraz czterech modeli wdrażania usług (**chmura prywatna**, **chmura wspólnotowa, chmura publiczna**, chmura **hybrydowa**); kluczowe technologie wspomagające obejmują: szybkie i wydajne sieci rozległe, wydajne oraz relatywnie niedrogie serwery (uwzględniając ich liczbę) oraz wysokowydajną wirtualizację sprzętu; Cechą chmury obliczeniowej jest współdzielona odpowiedzialność pomiędzy dostawcę i odbiorcę usług chmurowych.
Chmura prywatna		**ang**. **private cloud**. Model wdrażania chmury obliczeniowej, w którym infrastruktura jest udostępniana do wyłącznego użytku przez jedną organizację obejmującą wielu **Odbiorców usług**. Może być własnością organizacji, strony trzeciej lub ich kombinacji, bądź może być przez nie zarządzana i obsługiwana oraz zainstalowana w siedzibie tej organizacji lub poza nią.
Chmura publiczna		**ang**. **public cloud**. Model wdrażania chmury obliczeniowej, w którym infrastruktura jest udostępniana do użytku publicznego, może być własnością organizacji biznesowej, akademickiej lub rządowej lub ich kombinacji, bądź może być przez nie zarządzana i obsługiwana oraz jest zainstalowana w siedzibie dostawcy chmury.
Chmura wspólnotowa		**ang**. **community cloud.** Model wdrażania chmury obliczeniowej, w którym infrastruktura jest przeznaczona do wyłącznego użytku przez określoną grupę organizacji, mających wspólne założenia (m.in. misję, wymagania bezpieczeństwa, politykę, zgodność z regulacjami), może być własnością jednej lub więcej organizacji wchodzącej w skład grupy, strony trzeciej lub ich kombinacji, bądź może być przez nie zarządzana i obsługiwana i jest zainstalowana w siedzibie organizacji lub poza nią.

Nazwa	**Skrót**	**Opis**
Dostawca usługi w chmurze obliczeniowej		**ang. Cloud Service Provider**. Podmiot, który oferuje/świadczy usługi w chmurze. Niekwalifikowane użycie terminu Dostawca usług odnosi się do dowolnego lub wszystkich dostawców usług w chmurze, Operatora RChO lub innych niż Operator RChO.

Dostawca komercyjny		**ang. Commercial-Cloud Service Provider** Komercyjny Dostawca usług: odnosi się do organizacji niebędących jednostkami administracji publicznej oferującej usługi w chmurze **Odbiorcy usług** będącym podmiotem administracji publicznej w ramach przedsięwzięcia biznesowego, zwykle za opłatą z zamiarem osiągnięcia zysku.
Dostawca usług cyfrowych	**DUC**	Osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową *[szczegółowa def. W Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa]*
Elastyczność		**ang. rapid elasticity.** Usługi dostarczane z **chmury obliczeniowej** mogą być elastycznie konfigurowane i dostarczane, w niektórych przypadkach automatycznie, w celu szybkiego skalowania proporcjonalnie do popytu. Dla **Odbiorcy usług** udostępniane zasoby przetwarzania i usługi często wydają się być nieograniczone i mogą być przydzielane w dowolnej ilości i w dowolnym momencie.
Infrastruktura chmury		**Zasoby przetwarzania** stanowiące zbiór sprzętu i oprogramowania zgrupowanego w **pulę zasobów**, która umożliwia pięć zasadniczych cech przetwarzania w chmurze (patrz **chmura obliczeniowa**) zawierająca warstwę zarówno fizyczną (składającą się z zasobów sprzętowych, które są niezbędne do obsługi dostarczanych usług w chmurze obliczeniowej i zazwyczaj obejmują składniki serwera, pamięci masowej i sieci), jak i warstwę abstrakcji znajdującą się powyżej warstwy fizycznej (składającą się z oprogramowania rozmieszczonego w warstwie fizycznej, która posiada zasadnicze cechy chmury obliczeniowej);.
Infrastruktura jako usługa	**IaaS**	**ang. Infrastructure as a Service**. Usługa świadczona w **modelu chmurowym** zapewniająca **infrastrukturę chmury**, na której **Odbiorca usług** jest w stanie wdrożyć i uruchomić dowolne oprogramowanie (systemy operacyjne i aplikacje), nie zarządza ani nie kontroluje **infrastruktury chmury**, ale kontroluje systemy operacyjne, pamięć masową i wdrożone aplikacje oraz ewentualnie ma ograniczoną kontrolę nad wybranymi komponentami sieciowymi (np. zapór sieciowych).
Interoperacyjność		Zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych.
Katalog usług		**ang. Cloud Service Offering, CSO** Lista predefiniowanych i ustandaryzowanych usług infrastruktury informatycznej typu **IaaS**, **SaaS**, **PaaS** itd. (dla RChO zabezpieczona usługami bezpieczeństwa dostępnymi w ramach **RKB)** prezentowana poprzez portal WWW

		umożliwiająca samodzielne ich wykorzystanie przez **Odbiorcę usług**.
Kategoria Bezpieczeństwa	**SC**	**ang. Security Category** Charakterystyka informacji/danych lub systemu informatycznego oparta na ocenie potencjalnego wpływu utraty poufności, integralności lub dostępności takich informacji/danych lub systemu informatycznego na działania statutowe administracji publicznej, zasoby organizacyjne, osoby fizyczne, inne organizacje oraz bezpieczeństwo państwa.

Nazwa	**Skrót**	**Opis**
Model chmury obliczeniowej		Model proaktywnego świadczenia usług informatycznych. W tym modelu **infrastruktura chmury** dostarczana jest do użytkowników jako ustandaryzowana i prekonfigurowana usługa wymagająca od nich tylko niewielkiej, finalnej konfiguracji. Usługi dostępne są z **katalogu usług** w modelu samoobsługowym (patrz **self-service**) i rozliczane za ich użycie. Użytkownik nie kupuje infrastruktury informatycznej tylko ją użytkuje. Po stronie dostawcy usług pozostaje kwestia utrzymania określonego SLA, wydajności, dostępności oraz zabezpieczenia na wypadek awarii.
Model samoobsługowy	**Self-service**	Samoobsługa na żądanie. **Odbiorca usług** może samodzielnie użyć zasobów chmury, przygotowanych do automatycznej konfiguracji przez użytkownika, bez konieczności interakcji z obsługą techniczną dostawcy usług.
Network Operation Center	**NOC**	Centrum Zarzadzania Siecią. Dedykowany zespół specjalistów świadczący usługi zarządzania siecią **RChO**.
Ryzyko		Kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.
Szacowanie ryzyka		Całościowy proces identyfikacji, analizy i oceny ryzyka. Zgodnie z NIST SP 800-30 risk assessment jest to proces identyfikowania zagrożeń dla operacji organizacyjnych (w tym działań statutowych, funkcji, wizerunku, reputacji), zasobów organizacyjnych, osób, innych organizacji i Państwa, wynikających z działania systemu.
Odbiorca usług w chmurze obliczeniowej		1. Podmioty sektora finansów publicznych, o których mowa w art. 9 ust. 1-13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869); 2. inne państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego; 3. inne, niż określone w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, państwowe jednostki organizacyjne nieposiadające osobowości prawnej. Dotyczy podmiotów 1-3, które podpisały umowy o świadczenie usług **RChO**. Może wykorzystywać jeden lub wiele tenantów na potrzeby budowy systemów informatycznych.

Mitygacja ryzyka		Jest to narzędzie zarządzania ryzykiem obejmujące proces identyfikacji, oceny i redukcji ryzyka w celu minimalizacji negatywnych skutków zdarzeń niepożądanych. Na mitygację ryzyka składa się m.in. ustalanie priorytetów, ocena i wdrażanie odpowiednich zabezpieczeń / środków zaradczych zmniejszających ryzyko zalecanych w procesie zarządzania ryzykiem.
Operator RKB		Minister właściwy do spraw informatyzacji pełniący rolę Operatora Rządowego Klastra Bezpieczeństwa.
Oprogramowanie jako usługa	**SaaS**	**ang. Software as a Service**. Usługa świadczona w **modelu chmurowym** umożliwiająca **Odbiorcy usług** wykorzystanie aplikacji uruchomionej na **infrastrukturze chmury** dostarczanej przez dostawcę usług, dostępnej na różnych urządzeniach klienckich za pośrednictwem Odbiorcy usługi np.: przeglądarka internetowa lub klient aplikacji, oraz w przypadku której **Odbiorca usług** nie zarządza ani nie kontroluje **infrastruktury chmury**, a nawet parametrów konfiguracyjnych aplikacji, z wyjątkiem ograniczonych ustawień konfiguracji aplikacji specyficznych dla użytkownika.
Platforma jako usługa	**PaaS**	**ang. Platform as a Service**. Usługa świadczona w **modelu chmurowym** umożliwiająca **Odbiorcy usług** wdrożenie na **infrastrukturze chmury** aplikacji stworzonych przez siebie lub nabytych, które zostały przygotowane przy użyciu języków programowania, bibliotek, usług i narzędzi obsługiwanych przez dostawcę w przypadku której **Odbiorca usług** nie zarządza ani nie kontroluje **infrastruktury chmury** oraz systemów operacyjnych i baz danych, ale ma kontrolę nad wdrożonymi aplikacjami i, ewentualnie, nad ustawieniami konfiguracji dla środowiska udostępniania aplikacji.

Nazwa	**Skrót**	**Opis**
Prawo zamówień publicznych	**PZP**	Przepisy wynikające z Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. 1320) z późn. zm.
Publiczna Chmura Obliczeniowa	**PChO**	Chmura obliczeniowa dostępna w modelu **chmury publicznej** świadczona przez dostawców, spełniająca w szczególności wymagania w zakresie poufności, integralności i dostępności zdefiniowanych pod kątem zapewnienia bezpieczeństwa informacji administracji publicznej. Dostarcza usług infrastruktury informatycznej poprzez predefiniowany **Katalog usług** PChO.
Ramy Zarządzania Ryzykiem	**RMF**	**ang. Risk Management Framework** Sześciostopniowe, oparte na ryzyku podejście do bezpieczeństwa systemu informatycznego, którego celem jest zgodność z różnymi przepisami publicznymi. RMF zastępuje tradycyjne procesy certyfikacji i akredytacji C&A (NIST SP 800-37).
Rejestr publiczny		Ewidencja, wykaz, lista, spis albo inna forma ewidencji, służąca do realizacji zadań publicznych, prowadzona przez podmiot publiczny na podstawie odrębnych przepisów ustawowych np.: PESEL, CEiDG, SRP, CEPIK.

Rozliczanie usług		System zarzadzania **chmury obliczeniowej** automatycznie kontrolują i optymalizują wykorzystanie **zasobów przetwarzania**. Poprzez systemy pomiarowe kolekcjonują dane o ich wykorzystaniu w podziale na rodzaj (np.: przechowywanie, przetwarzanie, przepustowość i aktywne konta użytkowników). Wykorzystanie zasobów jest monitorowane, kontrolowane i raportowane, zapewniając przejrzystość rozliczenia zarówno dostawcy usług, jak i **Odbiorcy usług**. Rozliczenie wykorzystanej usługi może nastąpić na podstawie np.: płatności za użycie z ang. pay-per-use.
Rządowa Chmura Obliczeniowa	**RChO**	Chmura obliczeniowa typu **chmura wspólnotowa** dedykowana jednostkom administracji publicznej budowana w oparciu o **zasoby przetwarzania** oraz infrastrukturę teleinformatyczną, która pozostaje w dyspozycji podmiotów administracji publicznej, dostępna z **katalogu usług**. W jej skład wchodzą **ISR**, **IDR** i **RKB**.
Rządowy Klaster Bezpieczeństwa	**RKB**	Usługi bezpieczeństwa oraz środki techniczne stosowane do zabezpieczenie **RChO** będące implementacją wymagań **SCCO**.
Security Operation Center	**SOC**	Operacyjne Centrum Bezpieczeństwa. Centrum zarządzania bezpieczeństwem i obsługi incydentów. Dedykowany zespół specjalistów świadczący usługi zarządzania bezpieczeństwem i obsługą incydentów **RChO**.
Security Operation Center as Service	**SOC as a Service (SOCaaS)**	Usługa świadczona w modelu chmurowym oparta na subskrypcji, która zapewnia Odbiorcy usług m.in. całodobowe monitorowanie, wykrywanie zagrożeń i reagowanie na nie oraz obsługę incydentów.
Sieci rządowe		Sieci teletransmisyjne umożliwiające wymianę komunikacji pomiędzy publicznymi podmiotami krajowymi (GovNet), Unii Europejskiej oraz NATO (TESTA-NG), pozostające w gestii Ministra właściwego do spraw wewnętrznych oraz jednostek przez niego nadzorowanych.
Standardy Cyberbezpieczeństwa Chmury Obliczeniowej	**SCCO**	Zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych opracowany w oparciu o normy, standardy i metodyki uznane w obrocie profesjonalnym oraz w oparciu o rekomendacje Pełnomocnika rządu ds. cyberbezpieczeństwa.

Nazwa	**Skrót**	**Opis**
Systemy Rejestrów Państwowych	**SRP**	System informatyczny łączący najważniejsze polskie rejestry. Dzięki połączeniu rejestrów można załatwiać wybrane sprawy urzędowe, nie wychodząc z domu. System łączy pięć rejestrów: PESEL, Rejestr Dowodów Osobistych, Rejestr Stanu Cywilnego, System Odznaczeń Państwowych, Centralny Rejestr Sprzeciwów.

System Zapewnienia Usług Chmurowych	**ZUCH, System ZUCH**	System informatyczny pozwalający na klasyfikację systemu informatycznego administracji publicznej, wybór oraz zakup usług **PChO**, zgodnie z przepisami **PZP**.
Tenant		Architektura **chmury obliczeniowej** jest zbudowana w oparciu o tenanty (z ang. multi-tenant), które współdzielą **infrastrukturę chmury**. Każdy tenant to logicznie izolowana część **infrastruktury chmury** dedykowana do wyłącznego wykorzystania przez pojedynczego **Odbiorcę usług** i niedostępna dla innych **Odbiorców usług**. Tenant zawiera wszystkie usługi z **katalogu usług** wykorzystywane przez **Odbiorcę usług** wraz z ich konfiguracją oraz dane. Dostęp do tenantu jest możliwy dla uprawnionych użytkowników.
Wspólna Infrastruktura Informatyczna Państwa	**WIIP**	**Projekt WIIP** obejmuje dostarczanie infrastruktury informatycznej, jako usługi w modelu chmury obliczeniowej oraz zapewnienie bezpieczeństwa systemów teleinformatycznych tam uruchomionych poprzez budowę **RKB, RChO** i **PChO oraz udostępnienie Systemu ZUCH**. Celem projektu jest inicjalne dostarczenie **infrastruktury chmury** na potrzeby budowy **RChO,** udostępnienie **katalogu usług** oraz osiągnięcie odpowiedniego poziomu gotowości organizacyjnej. Może być rozumiany również jako projekt uchwały Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”.
Współdzielona odpowiedzialność		**ang**. **Shared Responsibility Model** Model bezpieczeństwa funkcjonowania **chmury obliczeniowej** opisujący ustalenia dotyczące odpowiedzialności dostawcy „Bezpieczeństwo chmury” i odpowiedzialności Odbiorcy usługi „Bezpieczeństwo w chmurze” w zakresie infrastruktury teleinformatycznej, środowiska przetwarzania, przetwarzania danych oraz usług.
Zarządzanie ryzykiem		skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka. Zgodnie z NIST SP 80037: risk management zarządzanie ryzykiem to program i procesy wspierające związane z działaniami instytucji (w tym działaniami statutowymi, funkcjami, wizerunkiem, reputacją), aktywami instytucji, osobami fizycznymi, innymi organizacjami i państwem, obejmujące: ustanowienie kontekstu dla działań związanych z ryzykiem; ocenę ryzyka; reagowanie na ryzyko raz określone; i monitorowanie ryzyka w czasie. *[NIST SP 80037: risk management]*.
Zintegrowana Infrastruktura Rejestrów	**ZIR**	**Infrastruktura chmury** dedykowana do obsługi systemów teleinformatycznych administracji publicznej, które mają kluczowe znaczenie dla realizacji zadań państwa o fundamentalnym znaczeniu budowana w ramach realizacji projektu **WIIP**. ZIR obsługuje **Rejestry Państwowe** dostępne z sieci wydzielonych i sieci o wysokim poziomie zaufania np. dedykowanych dla poszczególnych instytucji lub dedykowanej sieci. Ta część infrastruktury jest galwanicznie izolowana od **ISR**.

Załącznik 3 – Skróty

CSP	Cloud Service Provider (def. Dostawca usług)
DUC	Dostawca usług cyfrowych
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework (def. Ramy Zarządzania Ryzykiem)
SC	Security Category (def. Kategoria Bezpieczeństwa)
SP	Special Publication
VPN	Virtual Private Network

Załącznik 4 – Podstawowe Wymagania Bezpieczeństwa – Macierz zabezpieczeń

W osobnym pliku.

Załącznik 5 – Katalog zabezpieczeń

W osobnym pliku.