# Wymogi IRIS wobec dostawców, z wyłączeniem projektów radiowych

| | |
|---|---|
| Autor | Rohit Sunghay;<br>zmiany Małgorzata Meloch-Sobańska |
| Właściciel | IRIS TELECOMMUNICATION POLAND SP. Z O.O. |
| Organizacja | DZIAŁ ZAKUPÓW I ROZWOJU BIZNESU |
| Zatwierdził | PREZES ZARZĄDU – JAROSŁAW KASPERSKI |
| Rodzaj dokumentu | WYMAGANIA IRIS WOBEC DOSTAWCÓW Z WYŁĄCZENIEM PROJEKTÓW RADIOWYCH |
| Miejsce przechowywania dokumentu | DYSK I/INTRO/ZAKUPY |



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

# Spis treści

Wstęp - Cel, a) Zakres, b) Ocena i Weryfikacja wymogów IRIS wobec Dostawców





**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

# Wstęp

# Cel

Pojęcie “Dostawca” oznacza każdą stronę Umowy z IRIS Telecommunication Poland Sp. z o.o. (dalej IRIS), jak m.in. Dostawców, Współpracowników, Podwykonawców, Sprzedawców, Dostawców Usług, Partnerów, itd.

Pojęcie „dostawcy” pisane małą literą oznacza każdą stronę umowy (z wyjątkiem IRIS) z Dostawcą oraz dotyczy umów zawartych w łańcuch dostaw dla IRIS.

“Podwykonawca” oznacza dostawcę w sieci dostaw Dostawcy, który na podstawie umowy zawartej pomiędzy IRIS a Dostawcą został zgłoszony jako realizujący część zadań Dostawcy, określonych umową.

Cel Wymogów IRIS wobec Dostawcy (zwanych również IRIS-SR) jest trojaki:

**Po pierwsze**: w celu poinformowania o wymogach IRIS wobec Dostawców potencjalnych i istniejących w łańcuchu dostaw IRIS oraz wobec innych właściwych interesariuszy.

**Po drugie**: jako podstawa na potrzeby analiz kwalifikacji Dostawców i ryzyka prowadzonej działalności.

**Po trzecie**: jako ramy ciągłego rozwoju i doskonalenia się Dostawców.

IRIS-SR mają zastosowanie do wszystkich bezpośrednich, pośrednich produktów bądź usług dostarczanych IRIS przez Dostawcę oraz jego łańcuch dostaw.

Dostawca jest odpowiedzialny za zgodność z IRIS-SR w celu zmniejszenia ryzyk dla IRIS oraz zobowiązany jest do ciągłego doskonalenia możliwości biznesowych, wyników i konkurencyjności. Odpowiedzialność ta dotyczy również dostawców Dostawcy w łańcuchu dostaw dla IRIS. Na żądanie Dostawca wykaże IRIS zgodność z IRIS-SR i efektywne działanie systemów zarządzania Dostawcy.

## a. Zakres

„Matryca zastosowań” to podzbiór wymagań zawartych w IRIS-SR, mających zastosowanie do szczególnych wyników prac Dostawcy (produktów i/lub usług). Stanowi ona podstawę każdego badania zgodności. Dostawca będzie kaskadowo przenosił stosowne wymagania w matrycy zastosowań na swój łańcuch dostaw, odnosząc się do zakresu i wyników prac realizowanych na rzecz IRIS.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

Dostawca powinien dokonać wszelkich niezbędnych ulepszeń systemu zarządzania, aby uwzględnić zmiany w zakresie swojej współpracy z IRIS.

Dostawca powinien niezwłocznie zgłosić IRIS na piśmie wszelkie istotne odstępstwa lub braki w jego zdolności do przestrzegania IRIS-SR.

Wymogi zawarte w IRIS-SR podlegają zmianom i aktualizacji w celu zapewnienia ich aktualności w stosunku do standardów branżowych oraz zaspokojenia aktualnych wymogów klientów IRIS i prawidłowej realizacji procesu zarządzania bazą dostawców.

### b. Ocena i weryfikacja wymogów IRIS wobec Dostawców

IRIS ma prawo do zweryfikowania zgodności Dostawcy z aktualną wersją IRIS-SR, a Dostawca powinien udzielić IRIS niezbędnego wsparcia, dostępu do personelu/pracowników Dostawcy, istotnych dokumentów, informacji o lokalizacji swoich dostawców, niezbędnych do zweryfikowania zgodności w tym zakresie.

Zgodność Dostawcy z tymi wymogami będzie weryfikowana za pomocą ankiet Dostawcy, samooceny Dostawcy lub oceny/kontroli przeprowadzonych przez IRIS lub podmiot trzeci działający na zlecenie IRIS. W oparciu o wyniki analiz ryzyka prowadzonej działalności IRIS określi stosowaną metodę/metody weryfikacji. Wynikiem takich analiz będzie sprawozdanie z badania Dostawcy z zestawieniem niezgodności, ryzyk, najlepszych praktyk i obserwacji.

Dostawca powinien odnieść się do poszczególnych stwierdzonych niezgodności w ciągu 30 dni od dnia otrzymania Sprawozdania z badania Dostawcy lub zgodnie z harmonogramem uzgodnionym wspólnie między IRIS i Dostawcą, przedstawiając szczegółowy Plan działań naprawczych (CAP, *ang. Corrective Action Plan*).

Docelowy czas na zamknięcie wszystkich działań naprawczych to 90 dni od dnia otrzymania Sprawozdania z badania Dostawcy lub zgodnie z harmonogramem uzgodnionym wspólnie między IRIS i Dostawcą.

Dostawca powinien przekazać IRIS sprawozdanie z realizacji działań naprawczych (CAR, *ang. Corrective Action Response)* wraz z dowodami na wdrożenie działań naprawczych odnośnie do wszystkich stwierdzonych niezgodności. Według uznania IRIS, na miejscu może zostać przeprowadzona częściowa następcza ocena weryfikacji działań naprawczych.

Wynik kontroli Dostawcy IRIS zostanie uznany za “zatwierdzony”, gdy Dostawca spełni lub spełnia wszystkie mające zastosowanie wymogi. W przeciwnym razie wynik zostanie uznany za „niezatwierdzony”, dopóki wszystkie stwierdzone niezgodności i ryzyka nie zostaną rozwiązane w sposób zadowalający IRIS.

IRIS poinformuje Dostawcę na wskazany przez niego adres na piśmie lub elektronicznie z podpisem kwalifikowanym o wynikach oceny i następującym po nim zatwierdzeniu CAP, CAR oraz o usunięciu niezgodności.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

# 1. Odpowiedzialność kierownictwa

W tym rozdziale określono wymogi dotyczące wizji prowadzenia działalności przez Dostawcę, jego celów, polityk i strategii, wytycznych i procesów wdrożonych przez kierownictwo w celu zapewnienia realizacji wizji i osiągnięcia celów.

## 1.1 Wizja i strategia prowadzenia działalności

Dostawca powinien rozumieć status własnej organizacji i jej środowisko biznesowe, wizję tego, gdzie kierownictwo chciałoby, aby organizacja była w przyszłości oraz strategię rozwoju organizacji zgodnie z wizją. Kierownictwo ma odpowiedni plan pokazujący, jak zrealizować wizję i osiągnąć cele strategiczne.

## 1.2 Proces dotyczący strategii

U Dostawcy powinien funkcjonować proces dotyczący opracowania strategii, udostępniania jej w całej organizacji, jej komunikowania i skutecznego wdrożenia, jak również dalszej realizacji. Proces powinien obejmować kluczowych interesariuszy w organizacji, jeśli jest to konieczne do realizacji wspólnie uzgodnionych celów i zobowiązań.

Proces dotyczący strategii powinien opierać się na rzetelnej analizie środowiska biznesowego, konkurencji i łańcucha wartości, aby uchwycić kluczowych (wewnętrznych i zewnętrznych) interesariuszy, a także kluczowe możliwości biznesowe i związane z nimi ryzyka.

## 1.3 Wskaźniki dotyczące prowadzonej działalności i kontrola

Dostawca powinien posiadać zestaw kluczowych wskaźników efektywności (KPI) oraz system monitorowania i kontroli, co pozwoli na uwidocznienie kierownictwu postępów prowadzących do realizacji kluczowych celów strategicznych. System obejmie w sposób zrównoważony wszystkie strategiczne cele i poglądy różnych części organizacji.

## 1.4 Pomiary, analizy i zarządzanie udoskonaleniami

Dostawca powinien posiadać wskaźniki odnoszące się do jakości bądź wyników, mające zastosowanie do produktów lub usług dostarczanych IRIS. Objaśnienie, jak należy monitorować uzgodniony podzbiór wskaźników wraz z określeniem progów alarmowych powinno zostać włączone do umowy.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

## 1.5 Wskaźniki dotyczące produktu i świadczenia usług

Dostawca powinien posiadać wskaźniki odnoszące się do jakości bądź wyników, mające zastosowanie do produktów lub usług dostarczanych do IRIS. Objaśnienie, jak należy monitorować uzgodniony podzbiór wskaźników wraz z określeniem progów alarmowych powinno zostać włączone do umowy.

## 1.6 Wskaźniki dotyczące realizacji procesu

Dostawca powinien określić wskaźniki dla istotnych etapów procesów w celu mierzenia wyników oraz skutków kontroli i działań naprawczych. Takie wskaźniki będą powiązane z kluczowymi wskaźnikami efektywności (KPI) Dostawcy w celu oceny realizacji jego celów strategicznych.

## 1.7 Ciągłe udoskonalanie

Dostawca powinien poszukiwać możliwości ciągłego udoskonalania wyników i wdrażać stosowne projekty ukierunkowane na udoskonalanie. Dostawca powinien mierzyć rezultaty, posługując się wskaźnikami dotyczącymi wyników i jakości.

## 1.8 Karta wyników prowadzonej działalności

Dostawca powinien posiadać sposób (np. w formie zrównoważonej karty wyników czy dashboardów) monitorowania kluczowych celów strategicznych Dostawcy. Cele powinny być zrównoważone, aby dać ogólny obraz wyników. Wyniki powinny być oceniane i raportowane.

## 1.9 Przegląd operacyjny

Kierownictwo powinno przeprowadzać, w regularnych odstępach czasu, przeglądy operacyjne w celu zapewnienia ciągłego udoskonalania. Przeglądy powinny oceniać produkty pod kątem odnoszonych sukcesów i występujących problemów, przydatność i efektywność procesów, działania, możliwości poprawy i potrzeby zmian. Należy prowadzić dokumentację przeprowadzanych przeglądów operacyjnych.

## 1.10 Wytyczne dotyczące kluczowych aspektów i działań prowadzonej działalności

Dostawca powinien wdrożyć wytyczne dotyczące kluczowych aspektów i działań, wymagane zakresem prowadzonej działalności i prowadzoną współpracą. Kierownictwo zapewni, że wytyczne zostały zakomunikowane, przyjęte do wiadomości i wdrożone na wszystkich poziomach organizacji.

**Uwaga**: Przepisy prawa określają standardy na poziomie minimalnym, a nie maksymalnym, a Dostawców zachęca się do wykraczania poza zgodność z przepisami w obszarze etyki, zarządzania pracą, kwestii dotyczących środowiska, bezpieczeństwa i higieny pracy poprzez zobowiązanie się do spełniania odpowiednich standardów międzynarodowych (np. Międzynarodowej Organizacji Pracy czy konwencji ONZ) oraz do prowadzenia procesu ciągłego udoskonalania.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 1.11 Polityka dotycząca jakości

Dostawca powinien posiadać politykę dotyczącą jakości, definiującą pojęcie jakości oraz sposób zarządzania jakością.

### 1.12 Polityka zarządzania ryzykiem

Dostawca powinien posiadać politykę zarządzania ryzykiem, która określa, w jaki sposób Dostawca zarządza różnymi rodzajami ryzyka (prowadzona działalność, bezpieczeństwo i higiena pracy, bezpieczeństwo, środowisko, itp.). Polityka powinna promować identyfikację, analizę, kontrolę i monitorowanie ryzyk. Polityka powinna promować również działania mające na celu minimalizowanie prawdopodobieństwa wystąpienia zagrożeń związanych z przerwami w działalności oraz minimalizowanie skutków w przypadku zmaterializowania się ryzyka.

### 1.13 Polityka dotycząca praw własności intelektualnej (IPR)

Dostawca powinien określić Politykę dotyczącą praw własności intelektualnej ( ang.IPR *„Intellectual Property Rights*), w której respektowane będą prawa strony trzeciej oraz na podstawie której będzie zarządzał ryzykami powiązanymi z polityką IPR i podejmował stosowne działania odnośnie do roszczeń dotyczących naruszenia lub przywłaszczenia własności intelektualnej, aby chronić zarówno Dostawcę, jak i jego Klientów.

### 1.14 Polityka dotycząca wolnego i otwartego oprogramowania (WiOO) oraz innego oprogramowania osób trzecich

*(nie dotyczy)*

### 1.15 Polityka dotycząca bezpieczeństwa produktu, zabezpieczeń i odpowiedzialności

*(nie dotyczy)*

### 1.16 Postępowanie w biznesie i polityki

Dostawca powinien posiadać politykę dotyczącą postępowania etycznego lub kodeks, określający jak Dostawca rozumie wpływ własnej działalności biznesowej na kwestie etyczne, prawa człowieka i w jaki sposób nim zarządza.

Dostawca powinien posiadać również polityki regulujące kwestie zarządzania zasobami ludzkimi (regulujące kwestie rekrutacji i odejścia pracownika z organizacji, godzin pracy, wynagradzania i innych świadczeń, zapobiegania dyskryminacji, promowania równych szans, przeciwdziałania molestowaniu i nękaniu, pracy dzieci, pracy przymusowej, swobody zrzeszania się oraz odpowiedzialności pracowników), bezpieczeństwa i higieny pracy, ochrony środowiska i odpowiedzialnego zaopatrywania się w surowce mineralne, w stosownych przypadkach.

Kierownictwo powinno zapewnić, że kodeks postępowania etycznego, polityki i powiązane procesy zostaną zakomunikowane personelowi i przez niego zrozumiane. Należy sporządzać dokumentację z odbytych szkoleń.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

## 1.17 Organizacja i obowiązki, środowisko i etyka

Dostawca powinien określić role i obowiązki, w tym powołać przedstawiciela kierownictwa odpowiedzialnego za zapewnienie, że wymogi dotyczące systemu zarządzania w obszarze etyki, pracy, środowiska, bezpieczeństwa i higieny pracy oraz wymogi dotyczące zgodności produktów/usług zostały ustanowione, wdrożone i są utrzymywane. Dostawca powinien zapewnić zasoby ludzkie, techniczne i finansowe niezbędne do wdrożenia i kontroli systemów zarządzania operacjami, w tym umiejętności specjalistyczne, jeśli zajdzie taka potrzeba.

## 1.18 Bezpieczeństwo informacji

Dostawca powinien posiadać program bezpieczeństwa, realizowany przez wykwalifikowanego specjalistę ds. bezpieczeństwa informacji. Program bezpieczeństwa zapewni ramy dla utrzymania organizacji Dostawcy na pożądanym poziomie bezpieczeństwa, dzięki ocenie ryzyka i opracowywaniu działań mitygujących. Dostawca będzie stale rozwijać swój program bezpieczeństwa, aby zapewnić aktualne praktyki bezpieczeństwa. Dostawca zapewni, że wytyczne dotyczące bezpieczeństwa zostaną zakomunikowane jego pracownikom i przez nich zrozumiane.

## 1.19 Certyfikacja systemu zarządzania

*(nie dotyczy)*

## 1.20 System przeglądu umów

Dostawca powinien posiadać system przeglądu umów zapewniający, że wymogi Klienta są właściwie przekształcane w wewnętrzne wymogi organizacji Dostawcy dotyczące produktów lub usług. System przeglądu umów uwzględnia, w stosownych przypadkach, zapytania ofertowe, umowy zakupu, zamówienia, plany wewnętrzne i specyfikacje. Zapewnia, że wymogi są adekwatne, określone i udokumentowane, że wszelkie różnice między wymogami Klienta a wymogami i wewnętrznymi zostały rozwiązane, że wszystkie istotne ryzyka są zidentyfikowane i przeanalizowane oraz że obie strony, w tym ich interesariusze w zakresie badań i rozwoju oraz zaopatrzenia, podzielają wspólne rozumienie wymogów.

## 1.21 Program oceny satysfakcji Klienta

Dostawca powinien prowadzić Program zadowolenia Klienta, oceniający jakość produktu czy usługi za pomocą ratingów Klientów, ankiet Klientów, rozmów, itd. Kierownictwo będzie podejmowało działania w oparciu o powyższy Program.

## 1.22 Standardy rachunkowości

Sprawozdania finansowe powinny podlegać badaniu i udostępnieniu, najlepiej zgodnie z uznanymi standardami rachunkowości zgodnymi z obowiązującym prawem lokalnym. w celu zapewnienia wiarygodności sprawozdań finansowych.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 1.23 Budżety i plan biznesowy

*(nie dotyczy)*

### 1.24 Dopasowanie do potrzeb przedsiębiorstwa

Zasoby lokalowe Dostawcy powinny być w stanie należycie pomieścić wymagane wolumeny produkcji lub usług. Pomieszczenia powinny nadawać się do prowadzenia działalności i obejmować odpowiednio wydzielone obszary czyste, wydzielone obszary z kontrolą dostępu, klimatyzacją, itp.

### 1.25 Utrzymanie polityk i dowód na ich istnienie

*(nie dotyczy)*

# 2. Części składowe system zarządzania

W tym rozdziale określono zestaw procesów i procedur istotnych dla odbiorcy ze względu na potrzebę zapewnienia, że dostarczane produkty i/lub świadczone usługi są dobrej jakości.

### 2.1 System zarządzania jakością ((ang. *Quality Management System (QMS)*)

Dostawca powinien ustanowić, utrzymywać i stale doskonalić swoje procesy w systemie zarządzania jakością (QMS), mając na celu dążenie do lepszej jakości, ciągłe doskonalenie i zadowolenie Klienta. Procesy w systemie zarządzania jakością zapewniają, że wszystkie wyniki prac Dostawcy spełniają wymogi IRIS i jego Klienta.

QMS obejmuje swym zakresem m.in.:

- udokumentowane procesy z rolami i obowiązkami;
- narzędzia z danymi do ustalania wskaźników/kluczowych wskaźników efektywności i umożliwianie podejmowania decyzji w oparciu o dowody;
- zarządzanie relacjami z Klientami i komunikacja

### 2.2 Zarządzanie dokumentacją

Dostawca powinien posiadać system zarządzania dokumentacją, który obejmuje klasyfikację (dokumenty dotyczące procesów, produktów, administracyjne itp.) jego dokumentów QMS oraz ich hierarchię. QMS powinien obejmować również funkcje kontroli dokumentów w zakresie zatwierdzania dokumentów przed wydaniem, przeglądania i aktualizacji dokumentów, lokalizacji dokumentów i informacji, zapobiegania wykorzystywaniu nieaktualnych dokumentów oraz identyfikacji i kontrolowanej dystrybucji dokumentów dostarczonych przez IRIS i strony trzecie.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 2.3 Zarządzanie dokumentami

Dostawca powinien określić wewnętrzną i zewnętrzną dokumentację, wykazując zgodność z wymaganiami Klienta i wymogami prawnymi oraz dowody skutecznego wdrożenia swojego oprogramowania do zarządzania jakością (QMS). Przykłady takich dokumentów obejmują m.in. przeglądy wewnętrzne, sprawozdania z audytów, protokoły ze spotkań oraz testy materiałowe i produktowe oraz dane dotyczące kontroli. Dostawca powinien określić sposób gromadzenia, przechowywania, utrzymania i usuwania takich dokumentów. Wszystkie zapisy powinny być czytelne, łatwo rozpoznawalne i dostępne. Należy określić okres okres przechowywania dokumentów.

### 2.4 Audyty wewnętrzne

Dostawca powinien przeprowadzać okresowe audyty wewnętrzne przez wykwalifikowanych i/lub certyfikowanych audytorów. Audyty mają na celu sprawdzenie zgodności ze standardami, umowami i regulacjami oraz stwierdzenie wszelkich luk/niezgodności w politykach i/lub procesach. Do każdej luki należy przypisać działania naprawcze i zapobiegawcze w celu zajęcia się nią /rozwiązania tej kwestii Kierownictwo dokona przeglądu ustaleń audytu, stwierdzonych działań naprawczych i zapobiegawczych, docelowego harmonogramu w celu zajęcia się każdą niezgodnością, realizacji terminowego zamknięcia otwartych działań i weryfikacji skuteczności działań.

### 2.5 Działania naprawcze i zapobiegawcze *(ang. Corrective and Preventive Actions (CAPA)*

U Dostawcy i jego dostawców powinien funkcjonować proces ustalania i wdrażania działań naprawczych i zapobiegawczych (CAPA) w celu wyeliminowania pierwotnych przyczyn niezgodności, w tym m.in. problemów z dostawcami, reklamacji Klientów, problemów wewnętrznych, wad i nieefektywności. Działanie naprawcze ma na celu usunięcie przyczyny każdej niezgodności, a działanie zapobiegawcze zapobiega dalszemu powtórnemu wystąpieniu takiej niezgodności.

# 3. Zasoby ludzkie, bezpieczeństwo i higiena pracy oraz zarządzanie środowiskiem

W tym rozdziale określono katalog wymogów wobec Dostawców IRIS dotyczących zrównoważonego rozwoju (zasoby ludzkie, bezpieczeństwo i higiena pracy oraz zarządzanie środowiskiem), które są oparte na międzynarodowych standardach, takich jak Deklaracja Praw Człowieka ONZ, podstawowe konwencje Międzynarodowej Organizacji Pracy, standard społecznej odpowiedzialności SA 8000, norma dotycząca zarządzania bezpieczeństwem i higieną pracy ISO45001, norma dotycząca zarządzania środowiskowego ISO 14001, norma dotycząca odpowiedzialności społecznej ISO 26001, kodeks postępowania RBA oraz wytyczne JAC [współpraca w ramach audytu].

Aby w jak największym stopniu dostosować się do istniejących standardów, IRIS oczekuje od swoich Dostawców stosowania standardów określonych w wymaganiach zawartych w Kodeksie postępowania RBA, uzupełnionych o



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

**Kodeks postępowania Nokia dla podmiotów trzecich** oraz poniższe specyficzne wymagania IRIS dotyczące zrównoważonego rozwoju, które nie są objęte Kodeksem postępowania RBA).

### 3.1 Wymogi zawarte w Kodeksie postępowania RBA

Dostawca powinien przestrzegać najbardziej aktualnej wersji **Wymogów zawartych w Kodeksie postępowania RBA.**

## Zarządzanie zasobami ludzkimi

### 3.2 Godziny pracy i urlop

Dodatkowo do wymogu A3 w kodeksie postępowania RBA, dotyczącego godzin pracy, praca w godzinach nadliczbowych, jeśli dotyczy, jest dobrowolna i nie będzie wymagana regularnie. Pracownicy mają prawo do co najmniej 14 dni przysługującego w każdym roku, płatnego urlopu (dodatkowo do dni świątecznych) w roku, chyba że lokalne prawo nakłada wyższe wymagania.

### 3.3 Wynagrodzenie i świadczenia

Dostawca powinien szanować prawo personelu do **realizacji podstawowych potrzeb jednostki (living wage)** i zapewnić, że wynagrodzenie za normalny tydzień pracy, z wyłączeniem godzin nadliczbowych, zawsze będzie spełniało co najmniej minimalne normy prawne lub branżowe lub układy zbiorowe pracy, w zależności od tego, które z nich są wyższe. Dostawca zapewni swoim pracownikom ubezpieczenie społeczne i zdrowotne. Dostawca nie będzie wstrzymywał wypłaty jakiejkolwiek części wynagrodzenia swojego personelu ani innych świadczeń w celu zmuszenia takiego personelu do kontynuowania pracy dla organizacji. Dostawca nie będzie organizował praktyk zawodowych bez rzeczywistego zamiaru przekazywania umiejętności, a także nie będzie zawierał umów lub podejmował innych działań biznesowych, których celem jest uniknięcie wypełnienia zobowiązań wobec personelu zgodnie z obowiązującymi przepisami dotyczącymi pracy i zabezpieczenia społecznego.

### 3.4 Zarządzanie wynikami

Dostawca powinien posiadać system do zarządzania wynikami pracy pracowników i gwarantować ich uczciwą i obiektywną ocenę na podstawie określonych kryteriów i w określonych okresach czasu w celu ustalenia sposobu poprawy wyników.

### 3.5 Kompetencje i rozwój

Dostawca powinien zapewnić, że pracownicy posiadają wykształcenie, szkolenia i kompetencje wymagane na danym stanowisku i do realizacji określonych zadań oraz że pracownicy są świadomi obowiązywania polityk, swoich praw i obowiązków, powiązanych z wykonywanymi przez nich zadaniami. Na podstawie analizy kompetencji Dostawca powinien opracować plany szkoleniowe oraz wdrożyć je w celu zwiększenia i rozwoju możliwości personelu.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

## 3.6 Kanały przekazywania informacji zwrotnej i skarg

Dostawca powinien posiadać system, za pomocą którego pracownicy mogą przekazywać informacje zwrotne lub składać skargi dotyczące nieetycznego postępowania, niesprawiedliwego traktowania lub praktyk, naruszenia wartości organizacji, polityk i procedur albo przekazywać pomysły i sugestie dotyczące ulepszeń.

Kierownictwo powinno działać w oparciu o tę informację zwrotną i traktować ją jako poufną i anonimową. Zakaz działań odwetowych określony w rozdziale E6 kodeksu postępowania RBA, wersja 6.0, ma zastosowanie do wszystkich rozdziałów objętych tym kodeksem.

## 3.7 Procedura zakończenia zatrudnienia

Dostawca powinien zapewnić, że procedury zakończenia zatrudnienia są zgodne z obowiązującymi układami zbiorowymi pracy i przepisami. Okres wypowiedzenia jest taki sam dla pracownika i pracodawcy. Wobec odchodzących z miejsca pracy pracowników powinny zostać zrealizowane odpowiednie, zgodne z prawem działania, dotyczące na przykład procesu wypowiedzenia, ostatecznego rozliczenia wynagrodzenia, udokumentowania płatności dokonywanych na rzecz pracowników odchodzących z organizacji (w tym tych, którzy porzucają miejsce pracy). Dostawca powinien przetwarzać wszelkie dane osobowe przekazane przez pracownika ostrożnie, w sposób uczciwy, zgodny z prawem, chroniąc prywatność i prawa pracowników.

Dokumentacja pracowników, którzy odeszli ze organizacji, w tym dotyczące procesów ich rozliczeń, powinny być przechowywane przez okres co najmniej 12 miesięcy, chyba że obowiązujące przepisy o ochronie prywatności stanowią inaczej.

## 3.8 Umowa o zachowaniu poufności

Dostawca powinien zapewnić, że pracownicy wykorzystujący w pracy produkty czy projekty Nokia czy mający dostęp do specyficznej wiedzy, informacji o danych IRIS i/lub Nokia, albo do urządzeń/pomieszczeń IRIS i/lub Nokia podpiszą odrębną umowę o zachowaniu poufności lub taka umowa będzie częścią składową umowy o pracę. Dostawca zapewni, że pracownicy w pełni zrozumieli jej następstwa w praktyce.

## 3.9 Prawa człowieka I wykorzystanie technologii telekomunikacyjnej

Dostawcy powinni być świadomi i dostosować się do stanowisk przedstawionych w **Polityce Grupy Nokia w zakresie praw człowieka** dotyczących nadużywania technologii komunikacyjnych do naruszania praw człowieka. IRIS oczekuje, że technologia, którą dostarcza zgodnie z prawem i w dobrej wierze, będzie używana właściwie i zgodnie z prawem, zgodnie z obowiązkami w zakresie praw człowieka, wskazanymi przez naszych Klientów oraz obowiązujące przepisy prawa. Intencją IRIS nie jest naruszanie praw człowieka lub dostarczanie produktów czy usług naruszających prawa człowieka. Obowiązek ten rozciąga się na każdego Dostawcę, który obsługuje, konfiguruje, utrzymuje lub oferuje jakiekolwiek usługi związane z IRIS lub w jej imieniu. Dostawca zgłosi wszelkie naruszenia tych zasad za pośrednictwem istniejących kanałów składania skarg.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

## 3.10 Ochrona bezpieczeństwa i higieny pracy

Dodatkowo do rozdziału B w kodeksie postępowania RBA wskazuje się, iż Dostawca powinien powołać przedstawiciela kierownictwa wyższego szczebla w celu zapewnienia wszystkim pracownikom środowiska pracy spełniającego wymogi w zakresie bezpieczeństwa i higieny pracy. Dostawca powinien powołać i przeszkolić osoby odpowiedzialne za bezpieczeństwo i higienę pracy pracowników.

Dostawca przejmuje odpowiedzialność za bezpieczeństwo i higienę pracy pracowników pracujących poza siedzibą Dostawcy (np. w siedzibie Klienta). Odpowiedzialność ta rozciąga się także na wszystkich pracowników zatrudnionych w niepełnym wymiarze godzin i pracowników tymczasowych, zatrudnionych przez Dostawcę, w tym również na podstawie umów cywilnych.

## 3.11 Zasady IRIS ratujące życie

Dostawca powinien przestrzegać poniżej wskazanych zasad ratujących życie, zapewniając ich przestrzeganie i uświadamiając ich obowiązywania na wszystkich poziomach organizacji Dostawcy, a także Dostawca powinien monitorować zgodność podejmowanych działań z zasadami ratującymi życie:

- w DOWOLNYM pojeździe zapnij pasy w każdej sytuacji,
- Nie prowadź pojazdu mając osłabioną koncentrację lub będąc zmęczonym – rób przerwy co 2 godziny,
- Utrzymuj zawsze bezpieczną prędkość dostosowaną do drogi, natężenia ruchu i warunków pogodowych. Nie przekraczaj dozwolonej prędkości,
- Zawsze zabezpiecz siebie i swój sprzęt podczas pracy na wysokości,
- Zawsze upewnij się, że nikt nie przebywa poniżej twojego miejsca pracy na wysokości i wyznacz strefę niebezpieczną,
- Nie pracuj pod napięciem. Nie pracuj przy jakichkolwiek urządzeniach i instalacjach elektroenergetycznych, o ile nie zostałeś odpowiednio przeszkolony.

Dostawca powinien poinformować swoich pracowników o prawie do odmowy podjęcia pracy w przypadku niespełnienia którejkolwiek z zasad ratujących życie. Cały personel Dostawcy ma prawo odmówić wykonania zadania, które jego zdaniem jest niebezpieczne i naraża go na bezpośrednie ryzyko wystąpienia obrażeń.

# Zarządzanie środowiskowe

## 3.12 System zarządzania środowiskowego

*(nie dotyczy)*

## 3.13 Zarządzanie danymi o zawartości surowców

*(nie dotyczy)*



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 3.14 Wymogi dotyczące projektowania dla środowiska

*(nie dotyczy)*

### 3.15 Zawartość materiałów pochodzących z recyklingu

*(nie dotyczy)*

### 3.16 Gospodarowanie odpadami

*(nie dotyczy)*

### 3.17 Zarządzanie dostawcami Dostawcy i wymogi dotyczące zrównoważonego rozwoju

W ramach wymogów Dostawcy wobec dostawców w łańcuch dostaw dla IRIS, Dostawca powinien ustanowić na potrzeby swoich dostawców również wymogi środowiskowe (o ile dotyczy) oraz wymogi co do warunków pracy (np. dotyczące bezpieczeństwa i higieny pracy, etycznego postępowania, odpowiedzialnego zaopatrywania się w surowce mineralne). Dostawcy powinni ocenić wyniki dostawców i wyznaczyć cele dotyczące doskonalenia. Wymogi powinny być dostosowane do kodeksu RBA i wymogów IRIS wobec Dostawców. Jeżeli do usuwania odpadów wykorzystywany jest dostawca, Dostawca IRIS zapewnia, że dostawca posiada odpowiednie upoważnienie i licencję.

### 3.18 Badanie due diligence dotyczące odpowiedzialnego zaopatrywania się w surowce mineralne

*(nie dotyczy)*

# 4. Zarządzanie ryzykiem

W tym rozdziale określono wymogi dotyczące zdolności Dostawcy do zarządzania ryzykiem, tj. do identyfikowania, analizowania, zarządzania i monitorowania ryzyk, które mogą potencjalnie spowodować szkodę u Dostawcy lub IRIS. Dostawca ustanowi i będzie utrzymywać praktyki zarządzania ciągłością działania.

### 4.1 System zarządzania ryzykiem

Dostawca powinien posiadać system zarządzania ryzykiem (*ang. Risk Management System ,*RMS) w celu skutecznej identyfikacji, analizy, oceny ryzyka i postępowania z ryzykiem. Obejmuje to m.in. ryzyka biznesowe, takie jak ryzyko strategiczne, finansowe, operacyjne, handlowe, techniczne, jakościowe i związane z harmonogramem, a także ryzyka zewnętrzne, takie jak zagrożenia geograficzne, zagrożenia katastrofą naturalną, kontrola eksportu i odpowiedzialność za produkt. Dostawca powinien zastosować podobne wymogi w zakresie zarządzania ryzykiem do swoich własnych dostawców, mających związek z działalnością IRIS. Dostawca niezwłocznie powiadomi IRIS, jeśli ryzyko może potencjalnie wpłynąć na IRIS.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

## 4.2 Określenie odpowiedzialności za zarządzanie ryzykiem i praktyki

Dostawca będzie odpowiedzialny za identyfikację ryzyk. Statusy ryzyka, działania i właściciele powinny podlegać regularnym przeglądom. Dostawca powinien niezwłocznie poinformować IRIS o stanie wszystkich ryzyk, które mogą potencjalnie wpłynąć na działalność IRIS, przedstawiając jednocześnie odpowiednie działania ograniczające ryzyko i plany awaryjne. Dostawca powinien zapewnić IRIS pełne ujawnienie informacji związanych z ryzykami i działaniami ograniczającymi. Zarządzanie ryzykiem powinno być integralną częścią praktyk zarządzania i codziennej pracy.

## 4.3 Identyfikacja ryzyka i analizy

Dostawca powinien systematycznie identyfikować, analizować, dokumentować i informować o ryzykach, które mogą zagrozić osiągnięciu jego celów. Dostawca powinien przeanalizować prawdopodobieństwo i wpływ zidentyfikowanych ryzyk oraz ustalić priorytety w obszarze najważniejszych ryzyk na potrzeby analizy i opracowania planów ograniczenia ryzyka oraz planów awaryjnych.

## 4.4 Monitorowanie i zarządzanie ryzykami

Właściciel ryzyka jest odpowiedzialny za aktywne zarządzanie każdym pojedynczym ryzykiem, wdrażanie działań ograniczających ryzyko, monitorowanie ryzyka i skuteczności działań ograniczających oraz za komunikację. Dostawca powinien okresowo oceniać skuteczność działań w zakresie kontroli ryzyka.

## 4.5 Ciągłość działania i planowanie awaryjne

Dostawca powinien stosować systematyczne działania, aby chronić siebie i IRIS przed zakłóceniami w działalności prowadzonej z IRIS. Zakres planu ciągłości działania Dostawcy i zdarzeń awaryjnych obejmuje m.in. wszystkie krytyczne operacje biznesowe, siedziby/lokalizacje, procesy i jego łańcuch dostaw do IRIS. Plany będą okresowo testowane i weryfikowane.

Dostawca zapewni, że plany ciągłości działania są zatwierdzane przez kierownictwo wyższego szczebla, okresowo testowane i aktualizowane. IRIS może okresowo zażądać przeglądu planu Dostawcy i wyników testu weryfikacyjnego.

Dostawca powinien opracować swój plan ciągłości działania i reakcji na zdarzenia awaryjne, dostosowując je do wymogów dotyczących dostępności i maksymalnego czasu koniecznego na odzyskanie danych i wznowienie działania systemu w całości (RTO, ang. *Recovery-time objectives*), w zakresie dotyczącym współpracy z IRIS.

# 5. Bezpieczeństwo

W tym rozdziale określono wymogi dotyczące bezpieczeństwa informacji, obowiązujące Dostawcę i jego dostawców w łańcuchu dostaw dla IRIS.

Terminologia używana w tym rozdziale:



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

S/MIME = Bezpieczne / uniwersalne rozszerzenia poczty internetowej TLS = Transport Layer Security

Informacja krytyczna dla IRIS to wszelkie informacje lub zbiory informacji, uważane za mające największe znaczenie dla IRIS. Informacje krytyczne można zdefiniować na podstawie wartości, jaką wnoszą do organizacji, oraz skutków, jakie mogą być spowodowane w przypadku ich naruszenia. Przez "naruszenie" rozumiemy utratę, uszkodzenie lub wyciek informacji do nieuprawnionych osób.

Prototyp = wczesna wersja produktu, który zazwyczaj powstaje jako nowy produkt

Linia wdrożenia nowego produktu (NPI)

# Zarządzanie bezpieczeństwem

## 5.1 Ramy bezpieczeństwa

Dostawca powinien określić ramowe wymogi bezpieczeństwa informacji oraz wdrożyć i utrzymać odpowiednie organizacyjne i techniczne środki bezpieczeństwa informacji, aby zapewnić poufność, integralność i dostępność zasobów informacyjnych IRIS. Wymogi bezpieczeństwa opierają się na międzynarodowej normie bezpieczeństwa, takiej jak ISO/IEC 27001: 2013. Wymogi bezpieczeństwa informacji powinny obejmować polityki zatwierdzone przez kierownictwo, uzupełnione bardziej szczegółowymi wytycznymi, a także wyznaczone role i obowiązki związane z bezpieczeństwem. Wyznaczona osoba powinna pełnić funkcję punktu kontaktowego w sprawach bezpieczeństwa informacji wobec IRIS, a jej nazwisko podaje się IRIS na żądanie.

## 5.2 Klasyfikacja informacji

Dostawca powinien posiadać schemat klasyfikacji informacji i zasobów, oparty na wrażliwości informacji, który ukierunkowuje wdrożenie odpowiednich kontroli bezpieczeństwa. Wszystkie informacje IRIS są jasno określone; postępowanie z nimi jest oparte o wymogi klasyfikacyjne IRIS.

| Klasa tajności | Mogą być udostępniane | Kryteria | Przykłady |
|---|---|---|---|
| Wewnętrzne | Jedynie w obrębie IRIS/wykonawcą z NDA | Ujawnienie niewielkich części tych informacji opinii publicznej nie spowoduje znaczących szkód dla IRIS | Schemat organizacyjny, książka telefoniczna, dokumentacja polityki wewnętrznej, itp. |
| Poufne | Ograniczona dystrybucja w obrębie grupy | Ujawnienie tych informacji nieupoważnionym osobom spowodowałoby znaczące szkody dla IRIS | Projekt i specyfikacja produktu, dane finansowe, plan projektu, itp. |



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

| | | | |
|---|---|---|---|
| Tajne | Tylko dla wymienionych odbiorców | Ujawnienie tych informacji nieupoważnionym osobom spowodowałoby poważne ekonomiczne szkody, zagroziłoby podstawowym funkcjom biznesowym lub osobowym lub przyniosłoby szkodę wizerunkowi i reputacji spółki IRIS | Plany dotyczące strategii, informacje finansowe przed ich opublikowaniem, itp. |
| Osobowe | Brak klasy poufności IRIS, ochrona zgodnie z polityką Bezpieczeństwa danych osobowych w IRIS | Dla celów personalnych dozwolony jest uzasadniony osobisty użytek narzędzi dostarczonych przez spółkę. | Paski wypłaty, numery PESEL, karty identyfikacyjne, itp. |

## 5.3 Zarządzanie incydentami bezpieczeństwa/naruszeniami bezpieczeństwa

Dostawca powinien wdrożyć odpowiednie procedury reagowania na incydenty bezpieczeństwa i powołać wyznaczone osoby, które będą w odpowiednim czasie reagować i zapobiegać dalszym szkodom spowodowanym przez naruszenia bezpieczeństwa. Dostawca powinien powiadomić i eskalować takie zdarzenia, mające jakikolwiek wpływ na IRIS, za pośrednictwem oficjalnych kanałów we właściwym czasie (ale nie później niż 24 godziny od wykrycia incydentu) i wspólnie z IRIS uzgodnić niezbędne działania. Powiadomienie o wystąpieniu incydentu powinno zostać wysłane do osoby będącej głównym kontaktem w IRIS.

# Bezpieczeństwo osobiste i podwykonawców

## 5.4 Umowy o zachowaniu poufności

Dostawca zapewni, że umowy o zachowaniu poufności zostaną wdrożone wewnętrznie oraz dla ewentualnych dostawców przed przyznaniem im dostępu do informacji IRIS.

## 5.5 Bezpieczeństwo Podwykonawców (dostawców)

W przypadku, gdy odpowiednia umowa między IRIS a Dostawcą zezwala na korzystanie z Podwykonawców (dostawców), te wymogi mają również zastosowanie do takich Podwykonawców (dostawców). Dostawca jest odpowiedzialny za zapewnienie zgodności wymogów wobec Podwykonawców z wymogami IRIS.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 5.6 Procedury odejścia

Dostawca powinien zapewnić odpowiednią procedurę odejścia w przypadku zmian personelu na skutek rozwiązania umowy o pracę lub zakończenia działania w projekcie IRIS. Procedura określa zasady wyłączenia użytkownikowi dostępu do systemów IRIS oraz zwrotu użytkowanych zasobów IRIS.

### 5.7 Weryfikacja przeszłości pracowników

Dostawca powinien zapewnić weryfikację pracowników zatrudnionych przy projektach IRIS, jeśli zezwalają na to lokalne przepisy.

### 5.8 Świadomość bezpieczeństwa

Dostawca, przyjmując pracownika, powinien przeprowadzić szkolenie na temat zagadnień związanych z bezpieczeństwem informacji, a następnie powtórzyć szkolenie co najmniej raz w roku, dla wszystkich obecnych i nowych pracowników pracujących w projektach IRIS, aby zapewnić, że kładzie się należyty nacisk na praktyki pracy w zakresie bezpieczeństwa informacji. Szkolenie będzie oparte na materiałach poświęconych tej kwestii, opracowanych przez IRIS, o ile takie materiały zostaną dostarczone do Dostawcy. Na żądanie IRIS należy dostarczyć dowody odbycia szkoleń.

## Bezpieczeństwo fizyczne

### 5.9 Zabezpieczone środowisko pracy

Dostawca zapewni, że informacje IRIS są przetwarzane, przesyłane, przechowywane i udostępniane w zabezpieczonej i nadzorowanej lokalizacji i środowisku, w którym Dostawca jest w stanie zapobiec ujawnieniu informacji i zasobów IRIS nieuprawnionym osobom. W środowisku, w którym realizowany jest projekt IRIS, należy wdrożyć zasady czystego biurka i czystego ekranu. Dostawca jest zobowiązany do zawiadomienia IRIS o zmianie lokalizacji Dostawca. Dostawca w nowej lokalizacji zapewni zabezpieczenia, nadzór oraz środowisko dla informacji IRIS zgodnie z wymogami.

### 5.10 Kontrola dostępu

Dostawca powinien ograniczyć dostęp do środowiska pracy tylko do tych pracowników Dostawcy, którzy mają swój wkład w projekty IRIS. Dostawca powinien rejestrować próby dostępu, w tym prowadzić dzienniki wejścia i wyjścia do środowiska pracy. Dostawca powinien monitorować obszar roboczy przy użyciu środków fizycznych lub logicznych, aby zapewnić szybką reakcję na wtargnięcie do biura.

### 5.11 Polityka dotycząca gości

Dostawca powinien posiadać udokumentowaną politykę dotyczącą gości, a wszyscy goście powinni być rejestrowani i powinien im towarzyszyć pracownik Dostawcy. Dostawca uniemożliwi gościom dostęp do obszarów, w którym realizowany jest projekt IRIS lub obszarów, gdzie przetwarzane są nieopublikowane zasoby IRIS.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

## 5.12 Bezpieczne drukowanie i dysponowanie papierem

Dostawca powinien wykorzystywać dedykowane lub bezpieczne drukarki i niszczarki w celu zabezpieczenia informacji o projektach IRIS, sporządzonych na papierze. Dostawca zapewni, że wszystkie niepotrzebne materiały w wersji papierowej zostaną w każdym przypadku zniszczone przed opuszczeniem obszaru, w którym wykonywana jest praca na rzecz IRIS.

## 5.13 Reagowanie kryzysowe

Dostawca powinien posiadać udokumentowany i wdrożony aktualny plan reagowania kryzysowego na potrzeby projektów IRIS, koncentrujący się przede wszystkim na bezpieczeństwie osób, lokalizacji i zasobów. Dostawca powinien podać taki plan do wiadomości pracowników, a następnie powinien przekazywać tę informację o planie co najmniej raz w roku. Na żądanie IRIS należy przedstawić dowody.

## 5.14 Bezpieczeństwo w przypadku pożaru

Dostawca zapewni, że środowisko projektu IRIS i wszelkie związane z nim obiekty, w których mieszczą się ośrodki przetwarzania danych, będą wyposażone w odpowiednie środki wykrywania i zapobiegania pożarom. Obejmuje to czujniki dymu, alarmy przeciwpożarowe/ręczne ostrzegacze pożarowe, odpowiednie gaśnice i instalacje tryskaczowe. Dostawca będzie rejestrować i monitorować alarmy związane z dymem/pożarem, a informacja o wszelkich incydentach związanych z projektem IRIS będzie przekazywana do IRIS. Dostawca zapewni, że serwerownie lub pomieszczenia sieciowe będą miały odpowiednie możliwości gaszenia pożarów, zasilanie awaryjne, kontrole środowiska HVAC (wilgotność, wentylacja i klimatyzacja), podniesione podłogi i inne odpowiednie środki kontroli, o ile przepisy prawa nie stanowią inaczej.

# Postępowanie z krytycznymi informacjami i zasobami IRIS

## 5.15 Plan ochrony zasobów krytycznych

W stosownych przypadkach Dostawca powinien opracować udokumentowany plan ochrony informacji krytycznych w celu zajęcia się zidentyfikowanymi ryzykami i wdrożenia naprawczych środków ochrony informacji w środowisku Dostawcy, w którym przetwarzane są krytyczne informacje IRIS.

## 5.16 Zarządzanie prototypami

*(nie dotyczy)*

## 5.17 Bezpieczeństwo łańcucha dostaw

Dostawca powinien wdrożyć środki bezpieczeństwa łańcucha dostaw zgodne z międzynarodowymi standardami dotyczącymi łańcucha dostaw i przedstawić pisemne oświadczenie potwierdzające jego certyfikację w programie partnerstwa celno-handlowego przeciwko terroryzmowi (C-TPAT), status upoważnionego przedsiębiorcy (AEO), z uwzględnieniem wymogów dotyczących bezpieczeństwa i ochrony (AEO-F lub AEO-S) lub w równoważnym akredytowanym programie bezpieczeństwa Światowej Organizacji Celnej (WCO), zarządzanym przez zagraniczny



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

organ celny. Jeśli Dostawca nie jest certyfikowany, powinien niezwłocznie wykazać na piśmie, że spełnia wymogi celne dotyczące bezpieczeństwa łańcucha dostaw.

Nie dotyczy w przypadku działania łańcucha dostaw tylko na obszarze Polski.

## Bezpieczeństwo teleinformatyczne/cyber bezpieczeństwo

### 5.18 Zarządzanie tożsamością i dostępem

Dostawca powinien posiadać formalną procedurę zarządzania tożsamościami użytkowników i prawami dostępu do swoich systemów informatycznych oraz ograniczyć dostęp do informacji IRIS do tych pracowników, dla których taki dostęp jest niezbędny. Każdy użytkownik ma niepowtarzalną tożsamość użytkownika i tylko jedną tożsamość, której nie można dzielić z innymi użytkownikami.

### 5.19 Ścieżka audytu

Dzienniki dostępu użytkowników do danych IRIS powinny być gromadzone i przechowywane przez co najmniej 3 miesiące, chyba że lokalne przepisy stanowią inaczej. IRIS ma prawo wiedzieć, kto ma dostęp do danych IRIS.

### 5.20 Bezpieczeństwo urządzeń

Wszystkie urządzenia używane lub dodane do środowiska użytkownika końcowego Dostawcy powinny zostać zainstalowane przy użyciu standardowej, bezpiecznej konfiguracji. Aktualizacje i zmiany do systemu należy instalować niezwłocznie według zdefiniowanego procesu.

### 5.21 Ochrona przed złośliwymi kodami

We wszystkich systemach wykorzystywanych do pracy na rzecz IRIS należy zainstalować zautomatyzowaną, aktualną i funkcjonalną ochronę przed złośliwym kodem (jak antywirus i oprogramowanie szpiegujące/złośliwe oprogramowanie).

Jeśli na potrzeby komunikacji z IRIS wykorzystywana jest poczta elektroniczna, powinna istnieć możliwość wysyłania odpowiednio zaszyfrowanych wiadomości i należy stosować szyfrowanie typu od końca do końca lub gateway-to-gateway (S/MIME lub TLS).

Zdalny i bezprzewodowy dostęp Dostawcy będzie się odbywał zgodnie z określonymi politykami i procedurami, które będą chronić informacje IRIS przed podsłuchem. Na potrzeby zdalnego dostępu do zasobów IRIS należy wdrożyć uwierzytelnianie wieloskładnikowe.

### 5.22 Środki zabezpieczające

Dostawca zapewni, że kopie zapasowe będą wykonywane okresowo lub zgodnie z ustaleniami z IRIS i będą przechowywane w miejscu ognioodpornym (w lokalizacji lub poza nią) w celu zminimalizowania przerwy w



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

działalności i zapewnienia ciągłości działania. Kopie zapasowe należy również regularnie testować, aby zapewnić odpowiednią funkcjonalność oraz dostępność i integralność danych.

### 5.23 Szyfrowanie urządzeń i nośników wymiennych

Wrażliwe informacje IRIS, przechowywane na laptopach czy innych nośnikach wymiennych, jak pamięć USB, netbooki, smartfony, tablety i odtwarzacze przenośne, powinny być chronione dzięki odpowiedniemu szyfrowaniu.

### 5.24 Bezpieczne dysponowanie danymi

Wszystkie stare lub uszkodzone nośniki zawierające informacje IRIS należy skutecznie wyczyścić lub zniszczyć przed wycofaniem z eksploatacji lub ponownym użyciem.

### 5.25 Zwrot zasobów IRIS

Dostawca zobowiązuje się zwrócić wszystkie urządzenia będące własnością IRIS lub urządzenia, do których nadano dostęp oraz sprzęt IRIS (w tym m.in. tokeny do uwierzytelniania wieloskładnikowego, tokeny twarde, laptopy itp.) w ciągu piętnastu (15) dni lub wcześniej od:

(a ) wygaśnięcia lub rozwiązania umowy;

b) żądania IRIS zwrotu takiego mienia; lub

(c) dnia, od którego Dostawca (lub jego Dostawcy czy Przedstawiciele) przestał potrzebować takiego urządzenia.

# 6. Prawa własności intelektualnej i odpowiedzialność

W tym rozdziale określono wymogi związane z prawem własności intelektualnej (IPR), wolnym i otwartym oprogramowaniem (WiOO) oraz innym oprogramowaniem osób trzecich

### 6.1 Umowy dotyczące prawa własności intelektualnej I poufności:

Dostawca powinien zawrzeć i utrzymywać umowy ze wszystkimi osobami, w tym pracownikami i konsultantami wykonującymi prace na rzecz IRIS (dalej „Odpowiedni personel”). Taka umowa będzie zapewniała co najmniej, że:

(a) cały odpowiedni personel przydzieli lub przyzna Dostawcy wystarczające prawa własności intelektualnej w celu zapewnienia, że Dostawca może z kolei przydzielić, udzielić na zasadzie sublicencji lub w inny sposób udzielić IRIS uzgodnionych praw własności intelektualnej, i

(b) cały odpowiedni personel otrzymujący lub posiadający dostęp do poufnych i zastrzeżonych informacji IRIS jest świadom i przestrzega obowiązujących zobowiązań w zakresie poufności



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

i nieujawniania informacji, w tym ograniczeń w dostępie do informacji poufnych IRIS, ich wykorzystaniu, ujawnianiu i kopiowaniu.

### 6.2 Szkolenia i wdrożenie

Dostawca zapewni, że cały odpowiedni personel został przeszkolony w zakresie polityk i praktyk dotyczących praw własności intelektualnej, WiOO i oprogramowania osób trzecich, a dokumentacja z takich szkoleń będzie prowadzona.

# 7. Bezpieczeństwo i ochrona produktu, odpowiedzialność za produkt

W tym rozdziale zebrano wymogi, który realizacja ma umożliwić Dostawcy proaktywne identyfikowanie i ograniczanie potencjalnych ryzyk związanych z incydentami dotyczącymi bezpieczeństwa i ochrony, ekspozycją na działanie niebezpiecznych czynników, obrażeniami lub szkodami spowodowanymi przez produkt lub usługę.

Bezpieczeństwo i ochrona produktów to proces, rozpoczynający się od planowania i tworzenia produktu i/lub usługi, którego celem jest ciągłe minimalizowanie potencjalnych podatności i ograniczanie ryzyka związanego z ochroną.

### 7.1 Zarządzanie bezpieczeństwem i ochroną produktu oraz odpowiedzialnością za produkt

*(nie dotyczy)*

### 7.2 Szkolenie dotyczące bezpieczeństwa i ochrony produktu i świadomość

*(nie dotyczy)*

### 7.3 Metodologia bezpiecznego tworzenia produktów

*(nie dotyczy)*

### 7.4 Utwardzanie produktu; działania zabezpieczające oprogramowanie

*(nie dotyczy)*

### 7.5 Test zapewnienia jakości

*(nie dotyczy)*

### 7.6 Ocena podatności produktu i ocena bezpieczeństwa

*(nie dotyczy)*



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 7.7 Zarządzanie lukami w zabezpieczeniach produktu

*(nie dotyczy)*

### 7.8 Komunikowanie bezpieczeństwa produktu, alerty i aktualizacje

*(nie dotyczy)*

### 7.9 Ochrona przed odpowiedzialnością

Na żądanie IRIS, Dostawca przedstawi dowody, że podjął lub podejmie wszelkie niezbędne kroki w celu ochrony IRIS przed potencjalnym ryzykiem związanym z odpowiedzialnością za produkt lub usługę.

Dostawca zapewni, że w jego produktach lub usługach stosowane są wyłącznie bezpieczne materiały i komponenty, które zostały zatwierdzone przez odpowiednie władze.

### 7.10 Ubezpieczenie od odpowiedzialności

Dostawca posiada ważne ubezpieczenie odpowiedzialności cywilnej z tytułu prowadzenia działalności gospodarczej, wystawione przez towarzystwo ubezpieczeniowe prowadzące działalność na rynku polskim, z limitem odpowiedzialności nie niższym niż 500 000 PLN na jedno i wszystkie zdarzenia, z włączeniem odpowiedzialności cywilnej za dalszych Podwykonawców, obejmujące ochroną odpowiedzialność za gotowe komponenty i produkty lub usługi, w zakresie terytorialnym stosownym do charakteru współpracy z IRIS.

# 8. Zarządzanie cyklem życia

W tym rozdziale opisano wymogi odnoszące się do wszystkich etapów zarządzania cyklem życia produktu Dostawcy i/lub jego usług oraz powiązane z nimi procesy.

### 8.1 Zarządzanie cyklem życia produktu

*(nie dotyczy)*

### 8.2 Zarządzanie programem

*(nie dotyczy)*

### 8.3 Proces na potrzeby zapewnienia jakości

*(nie dotyczy)*

### 8.4 Procesy ze wskaźnikami

*(nie dotyczy)*



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 8.5 Planowanie wdrożenia nowego produktu (NPI)

*(nie dotyczy)*

### 8.6 Identyfikowalność produktu end-to-end

*(nie dotyczy)*

### 8.7 Zarządzanie utrzymaniem produktu, wsparciem i produktami wycofanymi z produkcji/eksploatacji

*(nie dotyczy)*

### 8.8 Proces zarządzania projektem

*(nie dotyczy)*

### 8.9 Plan i właściciel projektu

*(nie dotyczy)*

# 9. Rozwój produktu

W tym rozdziale określono wymogi dotyczące procesu Dostawcy dotyczącego rozwoju produktu.

### 9.1 Proces rozwoju produktu

*(nie dotyczy)*

### 9.2 Zarządzanie wymogami

*(nie dotyczy)*

### 9.3 Przegląd projektowania produktu i kwalifikacja

*(nie dotyczy)*

### 9.4 Projektowanie pod X

*(nie dotyczy)*

### 9.5 Zarządzanie zmianą

*(nie dotyczy)*



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 9.6 Przeglądy I kontrole

*(nie dotyczy)*

### 9.7 Testowanie

*(nie dotyczy)*

### 9.8 Zarządzanie integracją i wydaniami

*(nie dotyczy)*

### 9.9 Zarządzanie konfiguracjami

*(nie dotyczy)*

### 9.10 Zarządzanie usterkami

*(nie dotyczy)*

# 10. Zarządzanie dostawcami Dostawcy i nabywanie produktów/usług

W tym rozdziale opisano wymagania dotyczące sposobu zarządzania przed Dostawcę jego dostawcami w odniesieniu do całego zakresu prac dla IRIS.

### 10.1 Strategia dotyczące bazy Dostawców i wybór

Dostawca powinien posiadać dla swoich dostawców strategię dotyczące bazy dostawców, opartą na segmencie rynku/kategorii, wydatkach i zależności wolumenu od zarządzania ryzykiem.

Dostawca określi kryteria oceny, wyboru i zarządzania wynikami swoich dostawców. Kryteria są kompleksowe, np. (koszt, jakość, technologia) i zrównoważone w świetle wszystkich kryteriów. Dostawca powinien posiadać proces audytowania własnych dostawców.

Dostawca zapewni, że jego dostawcy będą przestrzegać IRIS-SR i umowy z IRIS.

Dostawca zapewni, że z dostawcami zawarto umowę zakupu i/lub umowę o świadczenie usług oraz ważne umowy o zachowaniu poufności.

Dostawca powinien posiadać program minimalizujący ryzyko związane z pojedynczymi źródłami dostaw. W przypadku źródeł pojedynczych Dostawca posiada plany ograniczania ryzyka i plany awaryjne (zapasy buforowe, długoterminowe zabezpieczenie dostaw).



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 10.2 Zarządzanie Dostawcami

Dostawca powinien posiadać dobrze zdefiniowany proces z rolami i obowiązkami w zakresie zarządzania dostawcami oraz jasno określoną kontrolą zakresu prac i wymogów dotyczących jakości, kosztów i czasu wprowadzenia na rynek wyników prac dostarczanych przez Dostawcę.

Dostawca powinien monitorować wyniki swoich dostawców za pomocą kluczowych wskaźników efektywności i okresowo przekazywać dostawcom informacje zwrotne.

W odniesieniu do zakresu prac IRIS, Dostawca zapewni, że jego dostawcy będą przestrzegać umów IRIS dotyczących poziomu usług utrzymania i wsparcia (SLA) oraz wymogów jakościowych.

### 10.3 Dokumenty zaopatrzeniowe i proces zarządzania zmianą

Dokumenty zaopatrzeniowe, posiadane przez Dostawcę, powinny zawierać wszystkie informacje niezbędne do określenia materiałów, produktów lub prac badawczo-rozwojowych, na które należy złożyć zamówienie. Informacje te obejmują szczegóły, takie jak nazwa pozycji, specyfikacja, poziom weryfikacji ilość, czas dostawy, cena i transport.

Dostawca powinien posiadać proces zapewniający, że wszystkie obowiązujące wymagania i zobowiązania umowne IRIS zostaną przeniesione na jego dostawców, a także powinien dokonać wdrożenia procesu zarządzania zmianą na potrzeby aktualizowania swoich dostawców w odniesieniu do wszelkich późniejszych zmian wymogów lub zobowiązań umownych.

Dostawca powinien posiadać proces śledzenia zmian zgłoszonych przez jego dostawców, analizowania i raportowania do IRIS wpływu zmian na wyniki prac dostarczanych do IRIS, w celu powiadomienia i na potrzeby ich zatwierdzenia. U Dostawcy powinien funkcjonować proces dostarczania aktualizacji i zmian do jego dostawców i śledzenia tych aktualizacji i zmian.

## 11. Popyt / Zarządzanie dostawami

W tym rozdziale opisano wymogi dotyczące sposobu zapewniania przez Dostawcę dostępności materiałów, komponentów, usług i zasobów niezbędnych do zapewnienia terminowej dostawy.

### 11.1 Proces planowania

*(nie dotyczy)*

### 11.2 Integracja systemów

*(nie dotyczy)*



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 11.3 Proces realizacji

*(nie dotyczy)*

### 11.4 Możliwości w środowisku SMI/SOI

*(nie dotyczy)*

### 11.5 Możliwość bezpośredniej dostawy do IRIS

*(nie dotyczy)*

### 11.6 Informacja o ograniczeniach popytu/łańcucha dostaw

*(nie dotyczy)*

# 12. Kontrola materiałów

W tym rozdziale opisano wymogi wobec sposobu, w jaki Dostawca postępuje z materiałami niezbędnymi do procesu produkcji czy procesu świadczenia usług.

### 12.1 Sprawdzenie materiałów przychodzących

*(nie dotyczy)*

### 12.2 Obchodzenie się z materiałami i ich przechowywanie

*(nie dotyczy)*

### 12.3 Kontrola zapasów

*(nie dotyczy)*

# 13. Projektowanie procesu wytwarzania, rozwój i zarządzanie

W tym rozdziale opisano wymogi dotyczące sposobu, w jaki Dostawca planuje, określa, kwalifikuje swoją produkcję/proces świadczenia usług i zarządza nimi.

### 13.1 Wprowadzenie produktu i przekazanie go na linię produkcyjną

*(nie dotyczy)*



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 13.2 Kwalifikacji procesu i kwalifikacja materiałów

*(nie dotyczy)*

### 13.3 Powiadomienie o zmianie produktu (PCN)

*(nie dotyczy)*

### 13.4 Zdolność procesu i kontrola

*(nie dotyczy)*

### 13.5 Urządzenia produkcyjne

*(nie dotyczy)*

### 13.6 Identyfikacja produktu

*(nie dotyczy)*

### 13.7 Postępowanie z produktem, przechowywanie i dostawa

*(nie dotyczy)*

### 13.8 Opakowanie produktu

*(nie dotyczy)*

### 13.9 Towary niebezpieczne

*(nie dotyczy)*

### 13.10 Utrzymanie porządku i postępowanie

*(nie dotyczy)*

### 13.11 Przeróbki i RMA

*(nie dotyczy)*

# 14. Zarządzanie kontrolą i testami na produkcji

W tym rozdziale określono wymogi wobec zarządzania kontrolą i testami na produkcji, lub wobec dostawy usług i związanego z tym wyposażenia.



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113

### 14.1 Uwolnienie produktu do Klienta

*(nie dotyczy)*

### 14.2 Dokumentacja dotycząca kontroli i testów

*(nie dotyczy)*

### 14.3 Kontrola niezgodnych materiałów/produktów

*(nie dotyczy)*

# 15. Odesłania

| | |
|---|---|
| CMMI | Capability Maturity Model® Integration Version 1.3,. Ocena procesu wytwórczego produktu i metodologia ulepszeń |
| P-CMM People | Capability Maturity Model (P-CMM) wersja 2.0, (http://www.sei.cmu.edu/cmm-p/) Ocena osób i metodologia udoskonaleń. |
| SA8000:2014 | Odpowiedzialność społeczna 8000 |
| TL 9000 | Podręcznik wymogów (wydanie 6.0) |
| BS25999 | Zarządzanie ciągłością działania, |

Koalicja Odpowiedzialności Społecznej Przemysłu Elektronicznego® (EICC®) Kodeks postępowania wytyczne JAC [współpraca w ramach audytu], Wytyczne dotyczące zrównoważonego łańcucha dostaw

Kodeks Postępowania RBA
https://www.responsiblebusiness.org/media/docs/RBACodeofConduct6.0_Polish.pdf

Kodeks postępowania trzeciej strony Nokia
nok2894-code-of-conduct-3rd-party-2024-eng-v2.pdf

Polityka Grupy Nokia w zakresie praw człowieka
https://www.nokia.com/about-us/company/leadership-and-governance/policies/



**IRIS TELECOMMUNICATION POLAND SP. Z O.O.** adres: al. marszałka Józefa Piłsudskiego 86, 92-202 Łódź; wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi Śródmieścia w Łodzi, XX Wydział Gospodarczy KRS, pod numerem KRS 0000684918, REGON: 367719600, NIP: 5213787067, kapitał zakładowy: 430 000 PLN, BDO 000211113