Wymagania w zakresie cyberbezpieczeństwa

Wymagania dla umów typu 3.:	**od 1 do 13**
Wymagania dla umów typu 2.:	**od 1 do 24**
Wymagania dla umów typu 1.:	**od 1 do 33**
Dodatkowe wymagania dla umów typu 1. w zakresie Zasobów specyficznych dla Umowy:	**od 34 do 67**

Spis treści

UWAGI WSTĘPNE

Niniejsze wymagania w zakresie Cyberbezpieczeństwa określają minimalne i standardowe ramy zasad, które muszą być przestrzegane przez dostawcę i jego ewentualnych podwykonawców w kontekście realizacji Umowy.

Zasady te muszą być określone w Planie zapewnienia bezpieczeństwa dla umów typu 1.
W przypadku Umów typu 2. lub typu 3. mogą one zostać określone w Planie zapewnienia bezpieczeństwa.

Wymagania w zakresie Cyberbezpieczeństwa nie mają pierwszeństwa przed stosowaniem (i) obowiązujących przepisów prawa i regulacji dotyczących Cyberbezpieczeństwa Systemów i danych oraz (ii) bardziej precyzyjnych i rygorystycznych obowiązujących zasad dotyczących Cyberbezpieczeństwa Systemów i danych, takich jak certyfikaty zgodności z normami takimi jak ISO, ETSI lub European Cybersecurity, mającymi zastosowanie dla Dostawcy, jego produktów, procedur i/lub usług, Zasad wewnętrznych oraz zasad uzgodnionych przez strony w inny sposób.

Należy przypomnieć, że niektóre Systemy informatyczne i ich Zasoby, ze względu na ich wrażliwość, mogą podlegać regulacjom, w szczególności w zakresie poufności (np. tajemnicy obrończej), obowiązków technicznych, ludzkich i organizacyjnych, kontroli i Audytu, kwalifikacji i akredytacji, zarządzania alarmowego i kryzysowego itp. Szczególne Zasady wewnętrzne (w tym polityka bezpieczeństwa Systemów informatycznych), jak również szczególne zasady kontraktowe będą również miały zastosowanie i będą nadrzędne w stosunku do niniejszych wymagań w zakresie Cyberbezpieczeństwa.

W odniesieniu do Technologii sztucznej inteligencji dodatkowe obowiązkowe procedury i postanowienia będą miały zastosowanie, gdy technologie te mają być wykorzystywane w ramach infrastruktury krytycznej (zwłaszcza w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557) lub wrażliwych czy kluczowych systemów i sieci firmy, lub tych podlegających szczególnym regulacjom w zakresie Cyberbezpieczeństwa. To samo będzie dotyczyć wszystkich systemów sztucznej inteligencji wysokiego ryzyka (w rozumieniu aktu w sprawie sztucznej inteligencji). Postanowienia zawarte w tych wymaganiach dotyczących sztucznej inteligencji nie mogą zastępować ani domyślnie obowiązywać w takich przypadkach.

Odniesienia do dostawcy należy rozumieć jako obejmujące dostawcę i jego podwykonawców, przy czym obowiązki dostawcy rozciągają się na Systemy informatyczne i Zasoby jego podwykonawców.

1 Terminy i definicje

Terminy zdefiniowane poniżej mają zastosowanie wyłącznie do wymagań w zakresie bezpieczeństwa – nie mogą być w żaden sposób używane ani wykorzystywane jako odniesienie w innych dokumentach Umowy.

Aktualny stan wiedzy: zasady i podstawowe pojęcia dotyczące bezpieczeństwa systemów informatycznych opisane w szczególności w normach (ISO, IEC) oraz tekstach opublikowanych przez oficjalne organy (ANSSI, NIST, ENISA).

Audyt: zestaw kontroli mających na celu zapewnienie zgodności dostawcy, jego usług lub towarów z obowiązkami prawnymi i umownymi w zakresie Cyberbezpieczeństwa. Rodzaje Audytów: organizacyjne, zgodności, konfiguracji i techniczne (testy penetracyjne, przegląd kodu itp.).

CERT (Computer Emergency Response Team) TotalEnergies: podmiot (Computer Emergency Response Team) odpowiedzialny za koordynację reakcji na incydenty informatyczne i Cyberbezpieczeństwa oraz ocenę cyberbezpieczeństwa jednostek firmy i ich dostawców. Zob. https://totalenergies.com/cert.

Centrum Operacyjne Bezpieczeństwa (SOC): Centrum Operacyjne Bezpieczeństwa (SOC) to scentralizowana funkcja w organizacji, która zatrudnia ludzi, procesy i technologie w celu ciągłego monitorowania i poprawy stanu bezpieczeństwa organizacji przy jednoczesnym zapobieganiu, wykrywaniu, analizowaniu i reagowaniu na Incydenty cyberbezpieczeństwa.

Cyberbezpieczeństwo: wszelkie techniczne i organizacyjne Środki niezbędne i proporcjonalne do ochrony Systemów informatycznych i Zasobów firmy, Zasobów specyficznych dla Umowy, Danych Klienta, użytkowników i stron trzecich (na które mogłyby mieć wpływ), przed zdarzeniami lub działaniami mogącymi zagrozić dostępności, autentyczności, integralności lub poufności Systemów informatycznych i Zasobów, a także Danych Klienta i usług, które oferują lub udostępniają.

Dane Klienta: dane, w tym dane osobowe, do których dostawca ma dostęp w ramach Umowy, a także dane (w tym logi i metadane) generowane przez Systemy.

Dostęp uprzywilejowany: upoważnienie do dostępu do zasobu w celu wykonania operacji administrowania zasobem (np. odczyt konfiguracji, modyfikacja konfiguracji, wykonanie polecenia zarezerwowanego dla administratora, usunięcie plików itp.).

Działania naprawcze: wdrożenie środków bezpieczeństwa lub środków w celu usunięcia błędów, wad, usterek lub awarii w cyberbezpieczeństwie.

Incydent cyberbezpieczeństwa: każde zaobserwowane zdarzenie mogące podważyć cyberbezpieczeństwo lub normalne funkcjonowanie Zasobu Systemu informatycznego (lub usługi zapewnianej przez funkcję Systemu informatycznego) klienta lub Zasobów specyficznych dla Umowy i mogące mieć wpływ na dostępność, integralność lub poufność odpowiedniego Zasobu lub Danych Klienta.

Klasyfikacja: klasyfikacja zasobu przez Klienta zapewnia Dostawcy zwięzłe wskazanie jego znaczenia i potrzeby odpowiedniego poziomu ochrony.

Komitet ds. bezpieczeństwa (SECCO): organ decyzyjny i monitorujący plany działania i wskaźniki cyberbezpieczeństwa.

Plan zapewnienia bezpieczeństwa (SAP): dokument opisujący warunki realizacji Umowy z punktu widzenia cyberbezpieczeństwa. Dokument ten opisuje wskaźniki cyberbezpieczeństwa, organizację cyberbezpieczeństwa i konkretne wdrożone środki cyberbezpieczeństwa.

Poziomy podatności: CERT definiuje i określa poziomy podatności (np. P0, P1, standardowy), które są zawarte w planie zapewnienia bezpieczeństwa, jeśli ma to zastosowanie.

Poważny incydent cyberbezpieczeństwa: każdy incydent cyberbezpieczeństwa skutkujący tymczasową lub trwałą utratą możliwości świadczenia usług na rzecz TotalEnergies.

Profil klasyfikacji: podejście do klasyfikacji, które polega na przypisaniu wartości odpowiadającej potencjalnemu wpływowi ryzyk mogących mieć wpływ na zasoby analizowane zgodnie z trzema rozpatrywanymi kryteriami.
Każdemu zasobowi przypisywany jest zatem poziom wrażliwości (od 0 = niski poziom wpływu do 4 = wysoki poziom wpływu) dla każdego z kryteriów: dostępność, integralność i poufność.

Przemysłowe systemy informatyczne (IIS): IIS to systemy informatyczne obejmujące systemy i składniki, które bezpośrednio wspomagają procesy produkcyjne, integralność, bezpieczeństwo i ochronę obiektów (systemy sterowania, zarządzanie laboratoriami, systemy zarządzania technicznego itp.).

Ryzyko (cyberbezpieczeństwa): ryzyko charakteryzuje się jako:

- zagrożenie lub złośliwe działanie pochodzenia wewnętrznego lub zewnętrznego na systemy informatyczne;
- zagrożenie lub działanie niezłośliwe, takie jak awaria, zaniedbanie lub błąd systemów informatycznych.

Silne uwierzytelnianie: uwierzytelnianie na podstawie co najmniej dwóch z poniższych:

- sekret znany wyłącznie użytkownikowi (hasło, PIN);
- obiekt posiadany przez użytkownika (karta haseł jednorazowych, karta inteligentna, klucz USB);
- cecha fizyczna użytkownika (odcisk palca, siatkówka oka, struktura dłoni lub inny element biometryczny).

System informatyczny: zorganizowany zbiór zasobów służących do przetwarzania danych i świadczenia usług. System informatyczny ma zasadnicze znaczenie dla działalności firmy. Obejmuje on System informatyczny przedsiębiorstwa (EIS) i Przemysłowy system informatyczny (IIS).

Systemy: termin odnosi się do systemów informatycznych klienta lub dostawcy wykorzystywanych w kontekście Umowy.

Systemy informatyczne przedsiębiorstwa (EIS): EIS to systemy informatyczne obejmujące usługi i aplikacje przeznaczone do zarządzania przedsiębiorstwem (automatyzacja czynności administracyjnych, zasoby ludzkie, relacje z klientami, finanse, podatki, zakupy itp.).

Środek (cyberbezpieczeństwa): środki zarządzania ryzykiem, które mogą mieć charakter administracyjny, techniczny, zarządczy lub prawny, w tym w szczególności polityki, procedury, wytyczne oraz praktyki lub struktury organizacyjne.

Technologia sztucznej inteligencji: każdy model lub system sztucznej inteligencji włączony, używany i/lub obsługiwany w ramach Umowy i wchodzący w zakres rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. (zwanego dalej „aktem w sprawie sztucznej inteligencji").

Umowa: odnosi się do wszystkich dokumentów regulujących stosunki kontraktowe między Dostawcą a Klientem dla określonej usługi.
Uwierzytelnianie: metoda weryfikacji tożsamości użytkownika uzyskującego dostęp do Systemu informatycznego.

Zagrożenie (cyberbezpieczeństwa): potencjalna przyczyna ryzyka cyberbezpieczeństwa, która może zaszkodzić systemowi informatycznemu lub organizacji.

Zasady wewnętrzne: odnoszą się do zasad klienta, w szczególności wszelkich zasad wewnętrznych i procedur specyficznych dla systemów informatycznych lub witryn klienta przekazywanych przez klienta dostawcy lub dostępnych z intranetu klienta.

Zasoby specyficzne dla Umowy: obejmuje Zasoby będące w gestii Dostawcy i jego podwykonawców, które są wdrażane specjalnie dla Umowy, w tym w szczególności stacje robocze pracowników zaangażowanych w Umowę oraz Zasoby dedykowane do realizacji Umowy przez Dostawcę.

Zasób (systemu informatycznego): obejmuje całość lub część środków, usług i procesów zaangażowanych w działanie Systemu informatycznego klienta, w szczególności takich jak aplikacje, dane, środki techniczne, sprzęt, sieci (lokalne, korporacyjne itp.). Określa się, że Zasoby obejmują środki, usługi i procesy dostawców, którzy uczestniczą w systemie informatycznym klienta, w tym dostawców usług w chmurze lub SaaS, dostawców usług odpowiedzialnych za usługi zarządzane lub outsourcowane itp.

Zdarzenie: informacja wygenerowana przez składnik systemu informatycznego, która jest rejestrowana w logu.

Złośliwy kod: każdy program napisany w celu wyrządzenia szkody systemowi komputerowemu lub sieci albo za ich pomocą.

2 Wymagania dotyczące umów typu 1., 2. i 3.

1. Podnoszenie świadomości w zakresie cyberbezpieczeństwa wśród personelu	Świadomość i szkolenia w zakresie cyberbezpieczeństwa
Dostawca musi prowadzić działania uświadamiające wśród personelu zaangażowanego w realizację Umowy (w tym podwykonawców), aby zapewnić, że są oni świadomi zasad Cyberbezpieczeństwa**,** które należy stosować.	

2. Zarządzanie incydentami związanymi ze Złośliwym kodem	Ochrona przed złośliwym kodem
Dostawca musi zdefiniować i wdrożyć procesy i procedury zarządzania Zagrożeniami i Złośliwym kodem. Dostawca jest zobowiązany do przestrzegania swoich kontraktowych i prawnych zobowiązań dotyczących zgłaszania Incydentów bezpieczeństwa do Klienta, w tym naruszenia danych osobowych lub nieosobowych.	

3. Zabezpieczenie urządzeń mobilnych wykorzystywanych na potrzeby Umowy	Bezpieczeństwo systemów mobilnych, stacji roboczych i sprzętu
Dostawca musi zapewnić istnienie konkretnych i odpowiednich Środków służących bezpieczeństwu jego urządzeń mobilnych wszelkiego rodzaju wykorzystywanych przez jego personel (i/lub personel jego podwykonawców) w kontekście realizacji Umowy.	

4. Zabezpieczenie nośników cyfrowych wykorzystywanych na potrzeby Umowy	Bezpieczeństwo nośników cyfrowych
Dostawca musi wdrożyć Środki ochrony nośników cyfrowych, na których są zapisywane i/lub archiwizowane (kopia zapasowa) Dane klienta wynikające z realizacji Umowy. Nośniki komputerowe muszą podlegać sformalizowanej Klasyfikacji i muszą być zgodne z rodzajem kopiowanych, zapisywanych i/lub archiwizowanych danych (kopia zapasowa). Spis nośników komputerowych musi być dostępny i aktualizowany. Nośniki kopii zapasowych i archiwizacji komputerowej muszą być zabezpieczone i chronione przed nielegalnymi działaniami i Ryzykami środowiskowymi. Transport nośników komputerowych musi podlegać udokumentowanej procedurze.	

5. Alert w przypadku Poważnego incydentu bezpieczeństwa	Zarządzanie Incydentami cyberbezpieczeństwa
Poważne incydenty bezpieczeństwa muszą zostać zgłoszone do CERT TotalEnergies w ciągu czterech (4) godzin od momentu, w którym Dostawca dowiedział się o nich, określając w szczególności charakter i zakres Poważnego incydentu bezpieczeństwa, udowodniony i potencjalny, a także wszelkie informacje umożliwiające Klientowi samodzielną ocenę konsekwencji. Dostawca aktywnie współpracuje z Klientem i regularnie aktualizuje i uzupełnia te informacje.	

6. Reagowanie na żądania jednostki kryzysowej Klienta	Zarządzanie Incydentami cyberbezpieczeństwa
Dostawca musi mieć komórkę zarządzania kryzysowego umożliwiającą mu jak najszybsze reagowanie na żądania jednostki kryzysowej Klienta.	

7. Test ciągłości działalności związanej z umową	Wymagania dotyczące ciągłości działania
Dostawca musi przeprowadzać systematyczne testy swoich rozwiązań organizacyjnych, ludzkich i technicznych w celu zapewnienia ciągłości działania i odzyskiwania po awarii, pod koniec ich wdrażania lub ewolucji, uzupełnione testami i regularnymi ćwiczeniami w celu oceny funkcjonowania wszystkich zdefiniowanych przez niego planów ciągłości działania i odzyskiwania po awarii.	

8. Sprzyjanie korzystaniu z narzędzi współpracy	Narzędzia współpracy i współdzielone przestrzenie robocze
W ramach wymiany z Klientem Dostawca musi w miarę możliwości korzystać z narzędzi do pracy zespołowej zaproponowanych lub udostępnionych mu przez Klienta. W niektórych przypadkach, w szczególności ze względu na poufność, Dostawca będzie zobowiązany do korzystania z narzędzi pracy zespołowej Klienta.	

9. Usuwanie wiadomości e-mail i dokumentów związanych z umową po zakończeniu Umowy	Narzędzia współpracy i współdzielone przestrzenie robocze
O ile nie określono inaczej w dokumencie kontraktowym, który ma pierwszeństwo przed niniejszymi wymaganiami, oraz o ile nie istnieje obowiązkowe zobowiązanie prawne, lub do celów certyfikacji produktu lub usługi będących przedmiotem Umowy, Dostawca musi usunąć ze swoich Zasobów, w tym Zasobów specyficznych dla Umowy, Dane klienta oraz wiadomości i dokumenty elektroniczne, w terminie maksymalnie jednego miesiąca od rozwiązania Umowy z jakiegokolwiek powodu.	

10. Przestrzeganie zasad dotyczących przesyłania wiadomości i narzędzi współpracy	Narzędzia współpracy i współdzielone przestrzenie robocze
Dostawca musi przestrzegać zasad dobrych praktyk związanych z komunikatorami i narzędziami do współpracy udostępnionymi mu przez Klienta.	

11. Deklarowanie Technologii sztucznej inteligencji używanych w umowie	Znajomość Technologii sztucznej inteligencji
Dostawca musi pisemnie zadeklarować klientowi, przed jakimkolwiek użyciem, Technologie sztucznej inteligencji, które zamierza wykorzystać w ramach Umowy, od momentu jej podpisania i w dowolnym momencie jej realizacji. To samo dotyczy przypadku jakiejkolwiek modyfikacji technologii sztucznej inteligencji podczas realizacji Umowy. Klient może sprzeciwić się na piśmie wykorzystaniu Technologii sztucznej inteligencji, bez konieczności uzasadnienia i bez odszkodowania lub rekompensaty dla dostawcy, przy czym Umowa będzie kontynuowana na pierwotnie uzgodnionych warunkach do jej zakończenia. Technologie sztucznej inteligencji dozwolone w dniu podpisania Umowy są wyczerpująco określone w załączniku z opisem usług.	

12. Zgodność Technologii sztucznej inteligencji używanych w umowie	Zgodność Technologii sztucznej inteligencji

Dostawca gwarantuje za siebie i swoich podwykonawców, że Technologie sztucznej inteligencji:

- nie zawierają żadnej zakazanej sztucznej inteligencji (w rozumieniu „aktu w sprawie sztucznej inteligencji") i że żadna zakazana sztuczna inteligencja nie była wcześniej używana w związku z Technologiami sztucznej inteligencji w realizacji Umowy;
- nie zawierają sztucznej inteligencji wysokiego ryzyka, z wyjątkiem uprzedniej pisemnej zgody Klienta i z zastrzeżeniem zastosowania szczególnych i uprzednich procedur, warunków umownych i technicznych przewidzianych przez akt w sprawie sztucznej inteligencji;
- są zgodne ze wszystkimi obowiązującymi przepisami, w tym z postanowieniami aktu w sprawie sztucznej inteligencji i są aktualizowane zgodnie ze zmianami w obowiązujących przepisach, w terminach ustawowych, bez dodatkowych kosztów dla Klienta;
- nie podlegały w ciągu ostatnich sześciu (6) miesięcy przerwom wynikającym z użycia jakiegokolwiek mechanizmu awaryjnego zapobiegającego wykonywaniu lub realizacji określonej funkcji przez Technologie sztucznej inteligencji;
- są wdrażane w ramach ścisłych specyfikacji, projektu oraz protokołów kontroli i nadzoru w celu ograniczenia dostępu do Technologii sztucznej inteligencji oraz danych szkoleniowych, testowych, weryfikacyjnych i doskonalących, oraz że nie było nieuprawnionego dostępu do algorytmu lub oprogramowania zawierającego Technologie sztucznej inteligencji lub do danych szkoleniowych, testowych, weryfikacyjnych używanych do szkolenia i/lub doskonalenia Technologii sztucznej inteligencji.

13. Monitorowanie operacji wykonywanych na Technologiach sztucznej inteligencji	Zgodność z obowiązkami dotyczącymi Technologii sztucznej inteligencji

Dostawca:

- dostarcza Klientowi całą dokumentację techniczną i funkcjonalną dotyczącą Technologii sztucznej inteligencji;
- wdraża wszystkie obowiązki określone w akcie w sprawie sztucznej inteligencji, w szczególności środki zapewnienia jakości, zarządzanie ryzykiem, nadzór ludzki, informację i przejrzystość;
- przechowuje informacje w czytelnej i łatwo dostępnej formie dla klienta lub organów regulacyjnych wyjaśniające wykonane operacje, uzyskane wyniki oraz podjęte lub ułatwione przez Technologie sztucznej inteligencji decyzje.

3 Dodatkowe wymagania dla umów typu 1. i typu 2.

14. Wyznaczenie inspektora ds. bezpieczeństwa	Zarządzanie cyberbezpieczeństwem
Dostawca wyznaczy osobę odpowiedzialną za bezpieczeństwo. Osoba ta będzie pojedynczym punktem kontaktowym ds. bezpieczeństwa przez cały okres obowiązywania Umowy. Musi być to osoba łatwo osiągalna w bezpieczny dla Klienta sposób, a środki komunikacji muszą zostać ustalone na początku Umowy.	

15. Wyznaczenie inspektora ds. Działań naprawczych	Zarządzanie cyberbezpieczeństwem
Dostawca musi wyznaczyć w ramach swoich zespołów osobę odpowiedzialną za stosowanie Działań naprawczych w odniesieniu do Klienta.	

16. Przedstawienie dowodów kwalifikacji	Certyfikaty dostawcy w zakresie cyberbezpieczeństwa
Dostawca musi przedstawić Klientowi wszelkie certyfikaty / akredytacje / oznaczenia / referencje potwierdzające jego kompetencje, w szczególności w dziedzinie cyberbezpieczeństwa, a także kompetencje jego pracowników i podwykonawców w zakresie Umowy. Należy również udostępnić dowody posiadania określonych kwalifikacji wymaganych w określonych ramach regulacyjnych.	

17. Utrzymanie kwalifikacji w zakresie cyberbezpieczeństwa	Certyfikaty dostawcy w zakresie cyberbezpieczeństwa
Dostawca jest odpowiedzialny za utrzymanie wymaganych certyfikatów, akredytacji i oznaczeń. Certyfikaty w zakresie Cyberbezpieczeństwa wymagane w ramach Umowy muszą być ważne co najmniej przez okres obowiązywania Umowy.	

18. Powiadomienie w przypadku utraty kwalifikacji	Certyfikaty dostawcy w zakresie cyberbezpieczeństwa
Dostawca musi powiadomić klienta tak szybko, jak to możliwe, a najpóźniej w ciągu siedmiu (7) dni roboczych, w przypadku utraty akredytacji, oznaczeń lub certyfikatu, niezależnie od tego, czy jest to certyfikat „firmy”, czy jeden lub więcej wymaganych certyfikatów mających zastosowanie do personelu, sprzętu, usług lub procesów dostawcy lub jego podwykonawców.	

19. Szkolenie personelu w zakresie cyberbezpieczeństwa	Świadomość i szkolenia w zakresie cyberbezpieczeństwa
Dostawca musi zapewnić, aby pracownicy wyznaczeni do realizacji Umowy (w tym interesariusze podwykonawców) nabyli wiedzę i umiejętności wymagane do wykonywania powierzonych im zadań oraz zagadnień związanych z Cyberbezpieczeństwem. Dostawca musi podjąć niezbędne działania szkoleniowe w celu utrzymania umiejętności wszystkich zainteresowanych pracowników i interesariuszy. Dostawca musi, na żądanie, przedstawić dowody istnienia programu podnoszenia świadomości i szkoleń.	

20. Zabezpieczenie stacji roboczych wykorzystywanych w ramach Umowy	Bezpieczeństwo systemów mobilnych, stacji roboczych i sprzętu
Dostawca musi zapewnić wzmocnienie zabezpieczeń stacji roboczych wykorzystywanych przez jego personel (i/lub podwykonawców) w kontekście realizacji Umowy, tak aby sprzęt ten nie stanowił wektora naruszenia bezpieczeństwa Zasobów wykorzystywanych do realizacji Umowy (np. kradzież sprzętu skutkująca ujawnieniem poufnych informacji lub utratą istotnych danych, rozprzestrzenianie Złośliwego kodu lub włamanie logiczne oraz nieuprawniony dostęp do wrażliwych Zasobów).	

21. Weryfikacja wdrożonych Środków cyberbezpieczeństwa	Projektowanie – implementacja – ewolucja Zasobów specyficznych dla Umowy
Dostawca musi przystąpić, przed dostawą, do technicznej weryfikacji wdrożonych Środków cyberbezpieczeństwa i zwrócić te wyniki Klientowi na koniec każdej kampanii kontrolnej. W stosownych przypadkach raport ten będzie zawierał informacje o odstępstwach od uprzednio zatwierdzonych specyfikacji bezpieczeństwa i zidentyfikowanych pozostałych Ryzykach dla bezpieczeństwa.	

22. Wdrożenie procesu zarządzania Incydentami cyberbezpieczeństwa	Zarządzanie Incydentami cyberbezpieczeństwa
Dostawca musi wdrożyć środki techniczne, ludzkie i organizacyjne w celu wykrywania, ostrzegania, wspierania i usuwania alertów Cyberbezpieczeństwa lub Incydentów cyberbezpieczeństwa, a w szczególności zgłaszania Klientowi Incydentów cyberbezpieczeństwa dotyczących Zasobów specyficznych dla Umowy lub Danych klienta wykorzystywanych w ramach Umowy, skutecznego reagowania zgodnie z charakterem i ważnością wykrytych Incydentów cyberbezpieczeństwa, ograniczania ich skutków oraz szybkiego i formalnego rozwiązywania wszystkich Incydentów cyberbezpieczeństwa.	

23. Ochrona danych klienta wykorzystywanych w kontekście Umowy	Narzędzia współpracy i współdzielone przestrzenie robocze
Dostawca musi zapewnić, że wszystkie dane i dokumenty dotyczące Klienta (w tym Dane klienta lub te wygenerowane przez usługę określoną w Umowie bądź dane inwentaryzacyjne) pozostają w dedykowanych i bezpiecznych środowiskach. Przesyłanie danych lub dokumentów poza te środowiska jest surowo zabronione. W szczególności dokumenty i wiadomości wymieniane w ramach Umowy nie mogą być przekazywane osobom trzecim bez uprzedniej zgody Klienta. Dostawca musi szyfrować wiadomości elektroniczne – dotyczące Danych klienta – wymieniane z klientem zgodnie z Aktualnym stanem wiedzy.	

24. Przestrzeganie najlepszych praktyk w zakresie bezpiecznego wytwarzania oprogramowania	Projektowanie wdrażanie – rozwój –
Programy i aplikacje wytworzone przez Dostawcę w ramach Umowy muszą być zgodne z Aktualnym stanem wiedzy w zakresie bezpieczeństwa wytwarzania oprogramowania komputerowego, a w szczególności z zaleceniami ENISA, ANSSI i OWASP (Open Web Application Security Project). Te najlepsze praktyki są opisane w Planie zapewnienia bezpieczeństwa i są zatwierdzane przez Komitet ds. bezpieczeństwa. Dostawca będzie również stosował zasady „security by design", „security by default", biorąc pod uwagę, w stosownych przypadkach, specyfikę narzuconą przez przetwarzanie danych osobowych. Klient może dostarczyć określony dokument dotyczący wymagań w zakresie cyberbezpieczeństwa w zależności od wdrożonych technologii.	

4 Dodatkowe wymagania dla umów typu 1.

25. Określenie ról i obowiązków w zakresie cyberbezpieczeństwa	Zarządzanie cyberbezpieczeństwem
Dostawca musi wdrożyć zarządzanie Cyberbezpieczeństwem w celu zagwarantowania poziomu bezpieczeństwa oczekiwanego przez Klienta i spełnienia wszystkich wymagań w zakresie Cyberbezpieczeństwa, ogólnych i szczegółowych, przewidzianych w Umowie i wszystkich jej załącznikach. W przypadku podwykonawstwa Dostawca musi ustanowić własne zasady zarządzania z podwykonawcami. Zarządzanie to opiera się w szczególności na uczestnictwie dostawcy w Komitecie ds. bezpieczeństwa (SECCO), który będzie spotykał się zgodnie z warunkami określonymi przez strony w Planie zapewnienia bezpieczeństwa (SAP). Tematy Komitetu ds. bezpieczeństwa będą koncentrować się na osiągnięciu poziomów bezpieczeństwa oczekiwanych przez Klienta, zaistniałych Incydentach cyberbezpieczeństwa, wszelkich odstępstwach bezpieczeństwa mających wpływ na Klienta, bieżących Incydentach cyberbezpieczeństwa, wynikach przeprowadzonych Audytów lub certyfikacji. Plany działania wynikające z analiz Ryzyka lub Audytów cyberbezpieczeństwa muszą zostać poddane przeglądowi podczas Komitetów ds. bezpieczeństwa. Procesy Działań naprawczych, wykrywania i reagowania muszą zostać zatwierdzone przez Komitet ds. bezpieczeństwa.	

26. Zapewnienie raportowania Działań naprawczych w zakresie Umowy	Zarządzanie Działaniami naprawczymi
Dostawca musi sporządzać i dostarczać, zgodnie z warunkami i częstotliwością określonymi w **Planie zapewnienia bezpieczeństwa**, raporty określone przez Komitet ds. bezpieczeństwa.	

27. Kontrola odpowiedzialności administratorów	Administrowanie Zasobami
Dostawca musi zapewnić, że jego personel (i personel jego podwykonawców) przypisany do funkcji administratorów ponosi odpowiedzialność za swoje działania wynikające z przyznanych uprawnień. Proces rozliczania administratorów z ich działań musi być sformalizowany (udokumentowany) i możliwy do prześledzenia.	

28. Zapewnienie bezpieczeństwa stacji roboczych administratorów	Zarządzanie stacjami roboczymi administratorów
Dostawca musi zapewnić, że stacje robocze używane do administrowania są utrzymywane w bezpiecznym stanie przez cały okres obowiązywania Umowy, a w szczególności aktualizowane i wolne od wirusów lub Złośliwego kodu, aby nie stanowiły Zagrożenia dla Systemu informatycznego Klienta.	

29. Ograniczenie dostępu do Internetu ze stacji roboczych administratora	Zarządzanie stacjami roboczymi administratorów
Konta administratorów i stacje robocze używane do administracji muszą być skonfigurowane w taki sposób, aby ograniczyć dostęp do Internetu (e-mail, przeglądanie) do ścisłych potrzeb niezbędnych do wykonania Umowy.	

30. Stosowanie zasady najmniejszych uprawnień dla administratorów	Zarządzanie stacjami roboczymi administratorów
Pracownicy Dostawcy (i jego podwykonawców) z uprawnieniami administratora muszą mieć osobiste i unikalne konta (bez kont współdzielonych) i przestrzegać rozdziału ról dla czynności administracyjnych. Uprawnienia administratora muszą być przydzielane i zarządzane zgodnie z zasadą najmniejszych uprawnień.	

31. Szyfrowanie danych stacji roboczej administratora	Zarządzanie stacjami roboczymi administratorów
Wszystkie nośniki danych używane do administrowania Systemem informatycznym Klienta muszą być szyfrowane. Sesje administratora muszą być automatycznie przerywane po określonym czasie bezczynności i zgodnie z Aktualnym stanem wiedzy.	

32. Zapewnienie fizycznego bezpieczeństwa stacji roboczych administratorów	Zarządzanie stacjami roboczymi administratorów
Dostawca musi zapewnić wdrożenie środków zabezpieczających przed kradzieżą i zapobiegających niepożądanemu podglądaniu. Operacje administratora w żadnym wypadku nie mogą być wykonywane w przestrzeni otwartej lub widocznej dla osób postronnych.	

33. Dostarczanie raportów dotyczących Incydentów cyberbezpieczeństwa	Zarządzanie Incydentami cyberbezpieczeństwa
Dostawca ma obowiązek aktualizować raporty dotyczące Incydentów cyberbezpieczeństwa i przekazywać je Klientowi zgodnie z częstotliwością i informacjami przewidzianymi w Planie zapewnienia bezpieczeństwa.	

5 Dodatkowe wymagania dla umów typu 1. z Zasobami specyficznymi dla Umowy

Poniższe wymagania mają zastosowanie wyłącznie w przypadku, gdy Umowa obejmuje Zasoby (wyposażenie) będące w gestii Dostawcy i jego podwykonawców, które są wdrażane specjalnie dla Umowy, w tym w szczególności stacje robocze pracowników zaangażowanych w Umowę oraz Zasoby dedykowane do realizacji Umowy.

34. Mapowanie zasobów specyficznych dla Umowy	**Znajomość Zasobów**
Dostawca musi zmapować Zasoby specyficzne dla Umowy wdrożone w ramach Umowy w formie schematów architektonicznych i musi utrzymywać spis wyszczególniający główne funkcje niezbędne do utrzymania bezpieczeństwa. Mapowanie to musi zostać zatwierdzone przez Komitet ds. bezpieczeństwa.	

35. Utrzymywanie aktualnego mapowania zasobów specyficznych dla Umowy	**Znajomość Zasobów**
Dostawca musi aktualizować mapowanie Zasobów specyficznych dla Umowy. Istotne zmiany muszą zostać przedstawione Komitetowi ds. bezpieczeństwa w wystarczającym i rozsądnym terminie przed ich wdrożeniem.	

36. Klasyfikacja zasobów specyficznych dla Umowy	**Znajomość Zasobów**
Dostawca musi zidentyfikować różne Zasoby specyficzne dla Umowy i ustalić, we współpracy z Klientem oraz w oparciu o system referencyjny Klienta, Klasyfikację tych zasobów.	

37. Przeszkolenie podmiotów w zakresie Klasyfikacji zasobów specyficznych dla Umowy	**Znajomość Zasobów**
Dostawca musi przeszkolić każdy podmiot zaangażowany w korzystanie z Zasobów specyficznych dla Umowy lub zarządzanie nimi w zakresie Profilu Klasyfikacji tych Zasobów. Administratorzy muszą opanować odpowiednie Środki cyberbezpieczeństwa.	

38. Analiza ryzyka cyberbezpieczeństwa dla zasobów specyficznych dla Umowy	**Zarządzanie ryzykiem cyberbezpieczeństwa**
Dostawca musi przeprowadzać i aktualizować analizę Ryzyka cyberbezpieczeństwa Zasobów specyficznych dla Umowy, w tym danych przetwarzanych przez te Zasoby, zgodnie ze wspólnie uzgodnioną metodą analizy. Dostawca musi być w stanie w każdej chwili dostarczyć szczegółowy raport na temat wszystkich zidentyfikowanych Ryzyk, sklasyfikowanych według wrażliwości, środków zapobiegania lub łagodzenia oraz ujawnić Ryzyka rezydualne.	

39. Zastosowanie planu działania w celu zmniejszenia zidentyfikowanych ryzyk	**Zarządzanie ryzykiem cyberbezpieczeństwa**
Dostawca musi wdrożyć, na własny koszt, plan działania w związku z analizą Ryzyk cyberbezpieczeństwa lub wynikami Audytu cyberbezpieczeństwa, aby zmniejszyć lub zapobiec wystąpieniu tych Ryzyk cyberbezpieczeństwa lub ograniczyć ich konsekwencje. Dostawca musi wdrożyć niezbędne Działania naprawcze po otrzymaniu powiadomień od Klienta w ramach swojego programu dotyczącego wycieku danych.	

40. Ochrona Zasobów specyficznych dla Umowy przed Złośliwym kodem	Ochrona przed złośliwym kodem
Dostawca musi wdrożyć dla swoich Zasobów specyficznych dla Umowy zabezpieczenie przed Złośliwym kodem.	

41. Przedstawianie okresowego raportu o stanie działań mających na celu zwalczanie Złośliwego kodu	Ochrona przed Złośliwym kodem
Dostawca musi regularnie przedstawiać Komitetowi ds. bezpieczeństwa ilościowy (kompletność) i jakościowy (skuteczność) raport z monitorowania środków zwalczania Złośliwego kodu wdrożonych w celu ochrony Zasobów specyficznych dla Umowy, zgodnie z częstotliwością określoną podczas pierwszego spotkania Komitetu ds. bezpieczeństwa.	

42. Zabezpieczenie bazy systemu zasobów specyficznych dla Umowy	Bezpieczeństwo baz systemów, stacji roboczych i sprzętu mobilnego
Dostawca musi wdrożyć niezbędne i odpowiednie Środki techniczne, ludzkie i organizacyjne w celu zapewnienia bezpieczeństwa Systemów bazowych (Systemów operacyjnych, oprogramowania pośredniczącego, aplikacji i powiązanych usług komunikacyjnych i bezpieczeństwa) Zasobów specyficznych dla Umowy. Środki te muszą umożliwiać zachowanie poufności, dostępności i integralności przetwarzanych danych.	

43. Ochrona danych zasobów specyficznych dla Umowy	Ochrona danych, bezpieczeństwo baz systemów, stacji roboczych i sprzętu mobilnego
Dostawca musi udokumentować i wdrożyć niezbędne i odpowiednie środki w celu zabezpieczenia administracji, utrzymania i eksploatacji baz Systemu (Systemów operacyjnych, oprogramowania pośredniczącego, aplikacji i powiązanych usług komunikacyjnych oraz bezpieczeństwa) Zasobów specyficznych dla Umowy.	

44. Ochrona sieci wykorzystywanej przez Zasoby specyficzne dla Umowy	Bezpieczeństwo sieci
Dostawca musi wdrożyć i aktualizować Środki bezpieczeństwa, niezbędne, odpowiednie i zgodne z Aktualnym stanem wiedzy, w celu zapewnienia bezpieczeństwa sieci wykorzystywanych przez Zasoby specyficzne dla Umowy, aby zapobiec lub ograniczyć skutki Ryzyk cyberbezpieczeństwa.	

45. Stosowanie procedury autoryzacji dostępu do zasobów specyficznych dla Umowy	Kontrole logicznego dostępu i autoryzacje
Zarządzanie I dostępem do Zasobów specyficznych dla Umowy, wdrożone przez Dostawcę na potrzeby Umowy, musi zostać opisane w Planie zapewnienia bezpieczeństwa (jeśli istnieje) lub w dokumencie przesłanym Klientowi przed rozpoczęciem świadczenia usług/dostaw i każdorazowo po jego aktualizacji. Dostęp do Systemu informatycznego Klienta podlega wyłącznie zasadom i procedurom Klienta.	

46. Audyt cyberbezpieczeństwa zasobów specyficznych dla Umowy	Audyty cyberbezpieczeństwa
Dostawca musi przeprowadzać Audyty cyberbezpieczeństwa Zasobów specyficznych dla Umowy. Audyty te dotyczą głównie zgodności z wymogami określonymi w niniejszym dokumencie. Mogą one również dotyczyć Środków cyberbezpieczeństwa mających zastosowanie do określonych przepisów, takich jak przepisy mające zastosowanie do przetwarzania danych osobowych. Audyty te nie wykluczają stosowania innych postanowień kontraktowych dotyczących Audytów Zasobów i Systemów informatycznych dostawcy, w tym Audytów w formie testów penetracyjnych / z udziałem „red teamu”. Audyty te są obowiązkiem Dostawcy, chyba że strony uzgodniły wcześniej inaczej.	

47. Przekazywanie wyników Audytów cyberbezpieczeństwa na zasobach specyficznych dla Umowy	Audyty cyberbezpieczeństwa
Wyniki Audytów przeprowadzonych przez Dostawcę na Zasobach specyficznych dla Umowy zostaną przekazane Klientowi. Certyfikat z Audytu, jak również podsumowanie raportu z Audytu oraz postępu Działań naprawczych i usprawniających, zostaną przekazane Klientowi bezpłatnie nie później niż w ciągu trzydziestu (30) dni roboczych od daty raportu z Audytu. Wszelkie Działania naprawcze i ulepszające zostaną podjęte na koszt Dostawcy.	

48. Usuwanie podatności w zasobach specyficznych dla Umowy	Zarządzanie działaniami naprawczymi
Dostawca musi zdefiniować i wdrożyć proces Działań naprawczych w celu usunięcia luk w zabezpieczeniach i błędów konfiguracji Zasobów specyficznych dla Umowy.	

49. Koordynowanie działań naprawczych w ramach terminów kontraktowych	Zarządzanie działaniami naprawczymi
Dostawca musi wdrożyć niezbędne środki w celu zastosowania Działań naprawczych dla zasobów specyficznych dla Umowy w terminach określonych w Planie zapewnienia bezpieczeństwa dla Poziomów podatności „krytyczny” lub „P0”, „pilny” lub „P1” oraz standardowy (domyślny). Działania naprawcze P0 i P1 są definiowane przez CERT TotalEnergies i przekazywane Dostawcy.	

50. Oddzielenie środowisk produkcyjnych systemów informatycznych od środowisk nieprodukcyjnych	Projektowanie – implementacja – ewolucja zasobów specyficznych dla Umowy
Dostawca musi zapewnić separację środowisk produkcyjnych Systemów informatycznych i nieprodukcyjnych Systemów informatycznych. Dane produkcyjne nie mogą być wykorzystywane w środowiskach nieprodukcyjnych bez uprzedniej pisemnej zgody Klienta.	

51. Określenie Środków cyberbezpieczeństwa w celu spełnienia wymagań dotyczących ewolucji zasobów specyficznych dla Umowy	Projektowanie – implementacja – ewolucja zasobów specyficznych dla Umowy
Dostawca musi określić i udokumentować Środki bezpieczeństwa, które mają zostać wdrożone w celu zapewnienia, w ramach projektów projektowania i/lub ewolucji Zasobów specyficznych dla Umowy, poziomów bezpieczeństwa i ciągłości usług wymaganych przez Klienta. Dostawca musi powiadomić Klienta o ewentualnej niemożności zaoferowania Środków cyberbezpieczeństwa spełniających żądane wymagania bezpieczeństwa.	

52. Ochrona fizycznego dostępu do zasobów specyficznych dla Umowy	Kategoryzacja stref bezpieczeństwa
Dostawca musi zapewnić stosowanie Środków bezpieczeństwa fizycznego dostosowanych do poziomu wrażliwości Zasobów specyficznych dla Umowy, w tym danych przetwarzanych na podstawie Umowy oraz zgodnie z obowiązującymi przepisami. Dostawca musi zapewnić ochronę fizycznego dostępu do różnych stref bezpieczeństwa, w których znajdują się Zasoby specyficzne dla Umowy, za pomocą stopniowanych i odpowiednich urządzeń w zależności od rodzaju zabezpieczanej strefy. Dostawca musi zapewnić funkcjonowanie Środków monitorowania i kontroli urządzeń ochrony dostępu fizycznego.	

53. Ochrona przeciwpożarowa zasobów specyficznych dla Umowy	Ochrona przed ryzykami środowiskowymi
Dostawca musi zapewnić wdrożenie Środków ochrony przeciwpożarowej w celu zabezpieczenia zasobów specyficznych dla Umowy. Środki te muszą obejmować w szczególności: - środki wykrywania pożaru; - środki gaszenia pożaru; - Środki do okresowej weryfikacji środków ochrony i gaszenia pożaru; - procedury, które należy wdrożyć w przypadku pożaru. Dostawca musi przekazać Klientowi listę wdrożonych Środków ochrony przeciwpożarowej.	

54. Ochrona przed szkodami spowodowanymi przez wodę	Ochrona przed ryzykami środowiskowymi
Dostawca musi zapewnić wdrożenie Środków ochrony przed wodą. Dostawca musi przekazać Klientowi listę wdrożonych Środków ochrony przed szkodami spowodowanymi przez wodę.	

55. Zapewnienie świadczenia niezbędnych usług dla Zasobów specyficznych dla Umowy	Ochrona przed ryzykami środowiskowymi
Dostawca musi zapewnić instalację i właściwą konserwację zasilania elektrycznego, klimatyzacji oraz ochronę Zasobów specyficznych dla Umowy.	

56. Przekazywanie zdarzeń wygenerowanych w wyniku Incydentu cyberbezpieczeństwa wpływającego na Zasoby specyficzne dla Umowy	Audyty Cyberbezpieczeństwa
W razie potrzeby **Komitet ds. bezpieczeństwa** może określić **Zdarzenia** budzące obawy oraz scenariusze wykrywania (logi, zdarzenia lub reguły detekcji), które należy przekazać do **SOC** Klienta, aby umożliwić wykrycie ich wystąpienia. **Zdarzenia** te, generowane przez **Zasoby specyficzne dla Umowy**, muszą zostać skierowane do systemów gromadzenia logów Klienta.	

57. Wdrożenie Centrum Operacyjnego Bezpieczeństwa (SOC)	Identyfikowanie i monitorowanie
Dostawca musi monitorować za pośrednictwem Centrum Operacyjnego Bezpieczeństwa (SOC) Zasoby specyficzne dla Umowy, które nie są zintegrowane z SOC Klienta. Dostawca musi ustanowić na początku obowiązywania Umowy protokół komunikacji między swoim SOC a SOC Klienta.	

58. Zgłaszanie Incydentów cyberbezpieczeństwa	Zarządzanie Incydentami cyberbezpieczeństwa
Dostawca musi powiadomić CERT TotalEnergies o wszelkich incydentach mających wpływ lub mogących mieć wpływ na Cyberbezpieczeństwo Zasobów specyficznych dla Umowy, w terminach i na warunkach kontraktowych lub wynikających z przepisów, przy czym termin ten jest domyślnie ustalony na maksymalnie dwadzieścia cztery (24) godziny od momentu, w którym Dostawca dowiedział się o Incydencie cyberbezpieczeństwa.	

59. Przesyłanie zdarzeń umożliwiających monitorowanie cyberbezpieczeństwa Zasobów specyficznych dla Umowy	Identyfikowanie i monitorowanie
Dostawca musi przekazać do Centrum Operacyjnego Bezpieczeństwa (SOC) Klienta, na pierwsze żądanie i w terminie dostosowanym do sytuacji, która to żądanie wygenerowała, wszystkie Zdarzenia związane z Incydentem cyberbezpieczeństwa wpływającym Zasoby specyficzne dla Umowy. Zdarzenia te muszą zostać skierowane do systemów gromadzenia logów Klienta.	

60. Wdrożenie zespołu Computer Emergency Response Team (CERT)	Zarządzanie Incydentami cyberbezpieczeństwa
Dostawca musi opisać w Planie zapewnienia bezpieczeństwa swoją organizację reagowania na Incydenty cyberbezpieczeństwa, równoważną zespołowi CERT (Computer Emergency Response Team) w monitorowaniu i reagowaniu na Incydenty cyberbezpieczeństwa dotyczące Zasobów specyficznych dla Umowy, które nie są zintegrowane z Centrum SOC ani zespołem CERT TotalEnergies. Dostawca wyznacza punkt kontaktowy zdolny do raportowania do CERT TotalEnergies. Dostawca musi ustanowić protokół komunikacji pomiędzy swoim zespołem CERT a CERT Klienta.	

61. Korzystanie z zapewnionych środków Uwierzytelniania	Administrowanie Zasobami specyficznymi dla Umowy
Dostawca będzie korzystał ze środków Uwierzytelniania udostępnionych przez Klienta w celu uzyskania dostępu do systemów informatycznych Klienta. Środki Uwierzytelniania w celu uzyskania dostępu do Zasobów specyficznych dla Umowy muszą zostać uprzednio zatwierdzone przez Klienta.	

62. Ochrona haseł dla Zasobów specyficznych dla umów	Administrowanie Zasobami specyficznymi dla Umowy
Personel przypisany do Umowy musi chronić swoje hasła i środki Uwierzytelniania zgodnie z metodami zatwierdzonymi przez Komitet ds. bezpieczeństwa i niezwłocznie alarmować Centrum Operacyjne Bezpieczeństwa (SOC) Klienta w przypadku naruszenia lub podejrzenia naruszenia.	

63. Zabezpieczenie przepływów operacji administrowania Zasobami specyficznymi dla Umowy	Administrowanie Zasobami specyficznymi dla Umowy
Dostawca musi korzystać ze środków i metod dostępu zatwierdzonych przez Komitet ds. bezpieczeństwa w celu administrowania Zasobami specyficznymi dla Umowy. Dostawca zobowiązuje się nie podejmować prób obejścia Środków cyberbezpieczeństwa wprowadzonych przez Klienta.	

64. Śledzenie działań administratora na zasobach specyficznych dla Umowy	Administrowanie Zasobami specyficznymi dla Umowy
Dostawca musi zapewnić, że działania kont administracyjnych używanych na Zasobach specyficznych dla Umowy są rejestrowane, przechowywane przez domyślny okres kolejnych dwunastu (12) miesięcy oraz że Zdarzenia podlegają Audytowi pod kątem podejrzanych działań.	

65. Zapewnienie dostępności Zasobów specyficznych dla Umowy	Wymagania dotyczące ciągłości działania
Dostawca musi ocenić Ryzyko niedostępności Zasobów specyficznych dla Umowy, które mogłoby być szkodliwe dla Klienta. Dostawca musi wdrożyć rozwiązania (techniczne, ludzkie i organizacyjne) obejmujące zidentyfikowane scenariusze niedostępności i umożliwiające zapewnienie minimalnego poziomu usług wymaganego przez Klienta w sytuacji kryzysowej oraz wznowienie świadczenia usług w warunkach zgodnych z progami tolerancji określonymi z Klientem.	

66. Awaryjna kopia zapasowa	Ciągłość działania
Dostawca musi wykonywać oddzielne produkcyjne kopie zapasowe i zapasowe kopie zapasowe obejmujące wszystkie Zasoby specyficzne dla Umowy (konfiguracja Systemu, sprzęt sieciowy i telekomunikacyjny, podstawowe oprogramowanie, aplikacje **i** Dane klienta). Dostawca musi zlecić wykonanie i przechowywanie kopii zapasowych (wykorzystywanych w ramach realizacji planów ciągłości działania) w miejscu wystarczająco oddalonym od miejsca produkcji, aby nie ucierpiało ono w wyniku katastrofy, która mogłaby mieć na nie wpływ. Dostawca musi zapewnić możliwość stałego dostępu do wszystkich awaryjnych kopii zapasowych niezależnie od miejsca ich przechowywania.	

67. Dokumentowanie ciągłości działalności związanej z umową	Wymagania dotyczące ciągłości działania
Dostawca musi przeprowadzać systematyczne testy swoich rozwiązań organizacyjnych, ludzkich i technicznych w celu zapewnienia ciągłości działania i odzyskiwania po awarii, pod koniec ich wdrażania lub ewolucji, uzupełnione testami i regularnymi ćwiczeniami w celu oceny funkcjonowania wszystkich zdefiniowanych przez niego planów ciągłości działania i odzyskiwania po awarii. Dostawca musi uzyskać pisemną zgodę klienta przed przeprowadzeniem jakichkolwiek testów i ćwiczeń opartych na częściowym lub całkowitym i zaprogramowanym wyłączeniu Zasobów specyficznych dla Umowy lub jego innych Zasobów niezbędnych do wykonania dostawy (w tym jakiegokolwiek przełączenia na systemy zapasowe). Wszystkie testy i ćwiczenia urządzeń do odzyskiwania po awarii i ciągłości działania muszą być zgodne z protokołami udokumentowanymi przez Dostawcę. Ich wykonanie musi być przedmiotem bilansu pokazującego wyniki zgodne z oczekiwaniami i/lub wykrytymi anomaliami, który dostawca musi przekazać Klientowi i który zostanie omówiony na posiedzeniu Komitetu ds. bezpieczeństwa.	

Koniec dokumentu.