Spis treści

1. Wprowadzenie

1.1 Klienci firmy BT oczekują, że firma BT i jej zewnętrzny łańcuch dostaw będą świadczyć swoje usługi z wykorzystaniem standardowych branżowych systemów zarządzania bezpieczeństwem informacji (ISMS). ISMS osoby trzeciej powinny obejmować infrastrukturę, sieci, sprzęt i systemy informatyczne w celu ochrony świadczonych usług i informacji o klientach BT/BT w zakresie usług. Niniejszy dokument określa wymogi bezpieczeństwa BT i ma zastosowanie do wszystkich osób trzecich pracujących dla lub w imieniu grupy BT, w tym Openreach, EE i Plusnet, zwanych dalej „BT" w pozostałej części dokumentu. Osoba trzecia zostanie poinformowana, które zestawy zabezpieczeń mają zastosowanie do usługi świadczonej na rzecz BT.

1.2 Niniejsze Wymogi dotyczące bezpieczeństwa stanowią uzupełnienie i pozostają bez uszczerbku dla wszelkich innych zobowiązań Osoby trzeciej wynikających z Umowy. Mają one na celu zapewnienie, że BT zachowuje kontrolę i nadzór nad swoją siecią i danymi użytkowników.

2. Wymogi dotyczące ograniczonego dostępu

2.1 Bez uszczerbku dla jakichkolwiek zobowiązań do zachowania poufności, w przypadku gdy Personel Osoby trzeciej ma dostęp do Informacji BT, Osoba trzecia musi:

2.2 dopilnować, aby Informacje BT nie były ujawniane Personelowi Osoby trzeciej ani aby Personel Osoby trzeciej nie uzyskiwał do nich dostępu, chyba że jest to konieczne do świadczenia Usługi; oraz

2.3 wdrożyć wszystkie systemy i procesy zarówno techniczne, jak i organizacyjne wymagane do ochrony Informacji BT (i) przed przypadkowym lub bezprawnym zniszczeniem oraz (ii) utratą, zmianą, nieuprawnionym ujawnieniem lub dostępem do Informacji BT zgodnie z Dobrymi praktykami branżowymi bezpieczeństwa.

3. Ogólne bezpieczeństwo informacji

3.1 Na uzasadnione żądanie Osoba trzecia udostępni BT kopie certyfikatów bezpieczeństwa i oświadczeń o zgodności istotnych dla Usługi w celu zilustrowania dowodów zgodności z niniejszymi Wymogami dotyczącymi bezpieczeństwa.

3.2 W przypadku istotnej zmiany w technologii lub branżowych standardach bezpieczeństwa bądź istotnych zmian w Usługach lub sposobie ich świadczenia, BT może wydać zmianę Umowy w okresie jej obowiązywania, jeśli zaistnieje potrzeba zmiany obowiązujących zestawów kontroli bezpieczeństwa. Osoba trzecia zastosuje się do uzgodnionej zmiany Umowy w rozsądnym terminie, biorąc pod uwagę charakter zmiany i ryzyko dla BT.

3.3 W przypadku jakichkolwiek istotnych zmian w Usługach lub sposobie ich świadczenia, Osoba trzecia musi dokonać przeglądu niniejszych Wymogów dotyczących bezpieczeństwa, aby upewnić się, że są one nadal zgodne ze wszystkimi obowiązującymi środkami kontroli bezpieczeństwa.

3.4 Jeśli Osoba trzecia podzleca obowiązki wynikające z Umowy, wówczas Osoba trzecia zapewni, aby wszystkie Umowy z odpowiednimi Podwykonawcami i ich Podwykonawcami zawierały pisemne warunki wymagające od Podwykonawcy

przestrzegania odpowiednich części niniejszych Wymogów bezpieczeństwa lub równoważnych wymogów bezpieczeństwa Osoby trzeciej.

3.5 3.5 Jeśli do świadczenia usługi zostanie wykorzystana osoba czwarta, która będzie przechowywać lub przetwarzać informacje BT, osoba trzecia musi uzyskać zgodę interesariusza BT na udostępnianie informacji. Osoba trzecia musi upewnić się, że ma stosunek umowny z osobą czwartą i musi upewnić się, że osoba czwarta działa zgodnie ze standardami branżowymi w zakresie bezpieczeństwa.

3.6 Informacje BT mogą być przechowywane tak długo, jak jest to konieczne do wykonania Umowy, po czym nie powinny być przechowywane dłużej niż maksymalnie dwa lata, chyba że inny okres przechowywania został uzgodniony między BT a Osobą trzecią lub jest wymagany przez obowiązujące przepisy prawa.

3.7 Jeśli Usługi są świadczone bezpośrednio na rzecz Kontraktu Rządu Wielkiej Brytanii, Osoba trzecia musi działać zgodnie z najnowszą wersją Cyber Essentials Plus – https://www.cyberessentials.ncsc.gov.uk/.

3.8 W przypadku, gdy Informacje BT będą przetwarzane lub przechowywane na morzu, Osoba trzecia musi poinformować BT o lokalizacjach geograficznych, a BT zastrzega sobie prawo do odrzucenia lokalizacji uznanych za obarczone wysokim ryzykiem.

Obsługa informacji BT

3.9 O ile interesariusz BT nie zaleci inaczej, wszystkie Informacje BT są klasyfikowane jako „Poufne". W przypadku danych osobowych lub wrażliwych danych osobowych należy zwrócić się o poradę do zespołu ds. ochrony danych i prywatności osoby trzeciej w przypadku, gdy wymagane są dodatkowe kontrole.

Poniższe środki kontroli bezpieczeństwa to „wymogi dotyczące obsługi głosowej", których zakres ogranicza się do komunikacji werbalnej.

3.10 Jeśli istnieje potrzeba omówienia, pokazania lub wymiany informacji BT przy użyciu platformy współpracy (np. Teams)

- -Należy się upewnić, że obecne są tylko osoby, które muszą znać te informacje.
- Jeśli zaangażowany jest wykonawca zewnętrzny, musi on mieć podpisaną umowę z Osobą trzecią lub mieć podpisaną umowę o zachowaniu poufności przed rozpoczęciem rozmów.
- Osoba trzecia musi zweryfikować, kto bierze udział w konferencji przed jej rozpoczęciem.

3.11 Jeśli istnieje potrzeba omówienia Informacji BT z kimś osobiście, przez telefon komórkowy lub standardową linię telefoniczną.

- Rozmowy nie mogą być prowadzone ani słuchane przez osoby, które nie muszą znać ich treści.
- Jeśli wymagana jest rozmowa z zewnętrznym wykonawcą, musi on mieć podpisaną umowę z Osobą trzecią lub przed rozpoczęciem rozmów musi zostać podpisana umowa o zachowaniu poufności.
- Informacje poufne lub wysoce poufne nie mogą być nagrywane na poczcie głosowej.

Poniższe środki kontroli bezpieczeństwa to „wymogi dotyczące postępowania z dokumentami pisemnymi", których zakres obejmuje materiały przechowywane w formie papierowej. Obejmuje to między innymi odręczne listy, protokoły, notatki i notatki. Obejmuje to również drukowane materiały elektroniczne, takie jak dokumenty robocze i raporty, gdy mają one format papierowy.

3.12 W przypadku przechowywania papierowych kopii informacji BT w siedzibie Osoby trzeciej, gdy nie są one używane, muszą być zabezpieczone w zamykanym obiekcie, z dostępem ograniczonym tylko do osób, które muszą zapoznać się z danym materiałem. Dokumentów nie wolno pozostawiać bez nadzoru.

3.13 Jeśli istnieje potrzeba wydrukowania, skopiowania lub powielenia Informacji BT, zastosowanie mają następujące środki kontroli bezpieczeństwa:

- -Z funkcji drukowania lub kopiowania można korzystać wyłącznie we własnych obiektach Osoby trzeciej.
- Kserokopie lub wydruki nie mogą być pozostawione bez nadzoru w miejscu drukowania i muszą zostać odebrane w momencie ich utworzenia.
- Jeśli drukarka lub kserokopiarka posiada pamięć, z której można przywołać i ponownie wydrukować skopiowane materiały, należy ją ponownie uruchomić w celu wyczyszczenia pamięci tak szybko, jak to możliwe.

3.14 W przypadku konieczności usunięcia kopii Informacji BT z siedziby Osoby trzeciej:

- O ile nie zostało to już uzgodnione w ramach zakresu prac, Osoba trzecia musi uzyskać udokumentowaną zgodę od interesariusza BT.
- -W przypadku zatwierdzenia, informacje nie mogą być możliwe do zidentyfikowania podczas transportu i muszą być przechowywane w anonimowej lub zwykłej teczce, torbie lub etui.
- Materiał nie może być pozostawiony bez nadzoru i musi pozostawać pod bezpośrednią kontrolą osoby transportującej materiał, zwłaszcza w środkach transportu publicznego.

3.15 Gdy papierowe kopie Informacji BT nie są już potrzebne, należy je zutylizować w następujący sposób:

- Kopie papierowe nie mogą być wyrzucane do zwykłych pojemników na odpady.
- -Jeśli używana jest niszczarka, musi ona spełniać minimalną normę P4 DIN66399.
- -Jeśli zatwierdzone niszczarki nie są dostępne, informacje należy wyrzucać do pojemników na odpady poufne.

W przypadku „informacji wysoce poufnych" zastosowanie mają dodatkowo następujące zasady:

- Odpady papierowe po rozdrobnieniu mogą być wyrzucane wyłącznie do pojemników na odpady poufne.
- -Informacje, które muszą zostać zniszczone na miejscu przez dostawcę, muszą uzyskać od niego certyfikat zniszczenia.

Poniższe środki kontroli bezpieczeństwa odnoszą się do Informacji BT w formacie elektronicznym.

3.16 W przypadku przechowywania informacji BT na komputerach PC lub laptopach innych firm obowiązują następujące zasady:

- -Dozwolone tylko na urządzeniach z szyfrowaniem dysku twardego (np. Bitlocker).
- Wszystkie dokumenty muszą być indywidualnie szyfrowane.
- Zarządzanie prawami do informacji (IRM) musi zostać zastosowane do dokumentu.
- Jeśli dostarczono, informacje muszą pozostać opatrzone etykietą klasyfikacji BT.

3.17 Podczas zapisywania dokumentu BT w wewnętrznej lokalizacji udostępniania plików w celu ogólnego przechowywania, współpracy lub udostępniania plików zastosowanie mają następujące mechanizmy kontroli bezpieczeństwa:

- Lokalizacja, w której przechowywane są materiały, musi mieć zastosowane uprawnienia dostępu, aby dostęp umożliwić tylko tym, którzy muszą zobaczyć lub użyć dokumentu.
- Jeśli dostarczono, informacje muszą pozostać opatrzone etykietą klasyfikacji BT.
- Wszystkie dokumenty muszą być indywidualnie szyfrowane.
- Zarządzanie prawami do informacji (IRM) musi zostać zastosowane do dokumentu.
- Jeśli w zakresie świadczonej usługi znajdują się materiały dotyczące PCI i kart płatniczych, nie mogą być one w żadnym momencie zapisywane w miejscach przechowywania plików.
- Jeśli konta gości są wymagane w celu zapewnienia dostępu zewnętrznemu kontrahentowi, muszą oni mieć podpisaną umowę z osobą trzecią lub umowę o zachowaniu poufności przed przyznaniem dostępu.

3.18 Jeśli istnieje potrzeba zapisania informacji BT na nośnikach wymiennych innych firm (np. pamięci USB), zastosowanie mają następujące środki kontroli bezpieczeństwa:

- Urządzenie musi być zaszyfrowane do tego samego poziomu, co dysk twardy.
- -W przypadku zgubienia lub kradzieży Osoba trzecia musi zgłosić incydent bezpieczeństwa.
- Osoba trzecia musi posiadać dowody uprzedniej zgody Interesariusza BT na przeniesienie „wysoce poufnych” materiałów na nośniki wymienne.
- Jeśli usługa obejmuje materiały PCI lub dane osobowe, nie wolno ich przechowywać na nośnikach wymiennych.
- Urządzenia przeznaczone do wsparcia i konserwacji nie mogą być używane do żadnych innych celów.

3.19 Informacji BT nie wolno przechowywać na komputerach osobistych, laptopach, nośnikach wymiennych ani urządzeniach przenośnych.

3.20 Informacje BT nie mogą być wysyłane lub automatycznie przekazywane z firmowego adresu e-mail Osoby trzeciej na osobisty adres e-mail lub zewnętrzne konto e-mail, chyba że jest ona zewnętrznym kontrahentem, który ma podpisaną umowę z Osobą trzecią lub NDA i jest wykorzystywany do świadczenia usługi.

3.21 Aby zminimalizować powierzchnię ataku i możliwości manipulowania ludzkim zachowaniem przez atakujących poprzez ich interakcję z przeglądarkami internetowymi i systemami poczty e-mail, należy wdrożyć procesy zapewniające, że dozwolone są tylko

w pełni obsługiwane przeglądarki internetowe i klienci poczty e-mail oraz odinstalować lub wyłączyć wszelkie nieautoryzowane wtyczki lub dodatki do przeglądarek lub klientów poczty e-mail.

3.22 Osoba trzecia musi posiadać kopie zapasowe w celu przywrócenia Informacji BT w ciągu 3 dni roboczych w przypadku ich uszkodzenia, utraty lub degradacji.

3.23 Podczas usuwania danych/informacji BT należy przechowywać pełną dokumentację dotyczącą przechowywania i usuwania danych, zapewniając ścieżkę audytu, dowody i śledzenie. Musi to obejmować:

- Dowód zniszczenia i/lub utylizacji (w tym data i zastosowana metoda).
- Dzienniki audytu systemu do usunięcia.
- Certyfikaty usuwania danych.
- Kto dokonał utylizacji (w tym partnerzy utylizacyjni / osoby trzecie lub wykonawcy).
- Raport zniszczenia i weryfikacji musi być generowany w celu potwierdzenia powodzenia lub niepowodzenia każdego procesu niszczenia / usuwania. (tj. proces nadpisywania musi dostarczyć raport zawierający szczegółowe informacje o wszelkich sektorach, których nie można było usunąć).

3.24 W przypadku utylizacji sprzętu, na którym znajdowały się dane/informacje BT, należy zapewnić ścieżkę audytu dla następujących typów sprzętu:

- Nośniki wymienne.
- Dyski.
- Taśmy zapasowe.
- Podzespoły komputerowe.

3.25 Musi istnieć pełna dokumentacja zapewniająca co najmniej następujące informacje dla ścieżki audytu:

- Nazwa aplikacji lub usługi korzystającej z tego urządzenia.
- Typ sprzętu, np. komputer stacjonarny, laptop, serwer, taśma, router itp.
- Liczba dysków twardych znajdujących się w urządzeniu (jeśli dotyczy).
- Sprzęt identyfikowany na podstawie numeru seryjnego.
- Części składowe sprzętu zidentyfikowane na podstawie numeru seryjnego.
- Pełne śledzenie zasobów całego sprzętu i części składowych przez cały cykl utylizacji sprzętu.
- Dowód zniszczenia i/lub utylizacji (w tym data i zastosowana metoda).
- Szczegółowe informacje na temat tego, kto dokonał utylizacji (w tym wszelkich partnerów w zakresie utylizacji / osób trzecich / wykonawców utylizacji odpadów).
- Należy wygenerować raport zniszczenia i weryfikacji, który potwierdzi powodzenie lub niepowodzenie każdego procesu recyklingu/sanityzacji lub niszczenia. Na przykład proces nadpisywania musi dostarczyć raport zawierający szczegółowe informacje o sektorach, których nie można było usunąć. Raporty te powinny zawierać informacje o pojemności, marce, modelu i numer seryjny nośnika.

Role i obowiązki

3.26 Każda osoba trzecia musi być świadoma i rozumieć wymogi tych środków kontroli bezpieczeństwa i jest odpowiedzialna za upewnienie się, że wszystkie osoby zaangażowane w świadczenie usług na rzecz BT znają i spełniają odpowiednie wymagania tego standardu.

Zarządzanie

3.27 Osoba trzecia musi posiadać ustanowione i spójne branżowe standardowe ramy bezpieczeństwa dla zarządzania bezpieczeństwem informacji i cyberbezpieczeństwem, które obejmują następujące elementy:

- Odpowiednie polityki i procedury w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa, które są zatwierdzane i komunikowane.
- Strategia bezpieczeństwa informacji.
- Odpowiednie wymogi prawne i regulacyjne dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa (w tym prywatności), które są zrozumiałe i zarządzane.
- Procesy zarządzania i zarządzania ryzykiem, które uwzględniają ryzyko związane z bezpieczeństwem informacji i cyberbezpieczeństwem.

3.28 Osoba trzecia musi zapewnić zdefiniowanie i wdrożenie odpowiednich ról i obowiązków w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa, które obejmują następujące elementy:

- Pełnoetatowy dyrektor ds. bezpieczeństwa informacji (lub jego odpowiednik), który zajmuje odpowiednio wysokie stanowisko i jest odpowiedzialny za program bezpieczeństwa informacji.
- Grupa robocza wysokiego szczebla, komitet lub równoważny organ, który koordynuje działania związane z bezpieczeństwem informacji u Osoby trzeciej, któremu przewodniczy odpowiednio starszy członek personelu i który spotyka się regularnie.
- Specjalistyczna funkcja bezpieczeństwa informacji z odpowiednimi i zdefiniowanymi rolami i obowiązkami.

3.29 Osoba trzecia musi zapewnić, że istnieje indywidualna odpowiedzialność za informacje i systemy poprzez zapewnienie, że istnieje odpowiednia własność krytycznych środowisk biznesowych, informacji i systemów oraz że jest ona przypisana do odpowiednich osób.

3.30 Osoba trzecia musi dopilnować, aby BT została powiadomiona (na piśmie) tak szybko, jak jest to prawnie możliwe, jeśli Osoba trzecia podlega fuzji, przejęciu lub jakiejkolwiek innej zmianie własności.

Zarządzanie incydentami

3.31 Osoba trzecia musi mieć ustanowione i spójne ramy zarządzania incydentami, aby zapewnić, że incydenty są odpowiednio zarządzane, ograniczane i łagodzone i obejmują następujące elementy:

- Upewnienie się, że personel zna swoje role i kolejność działań, gdy potrzebna jest reakcja.
- Zapewnienie zgodności zgłaszanych incydentów z ustalonymi kryteriami.
- Upewnienie się, że wpływ incydentu jest zrozumiały.
- Zapewnienie, że badania kryminalistyczne są wykonywane w razie potrzeby wewnętrznie lub przez wyspecjalizowaną jednostkę.
- Zapewnienie, że wnioski wyciągnięte z incydentów są włączane do najlepszych praktyk.
- Zapewnienie, że informacje związane z incydentem mającym wpływ na BT są traktowane jako „poufne".

3.32 Osoba trzecia podejmie wszelkie uzasadnione kroki w celu zapewnienia wyznaczenia odpowiedniej osoby (osób) i uczynienia jej odpowiedzialną za Punkt kontaktowy w zakresie ryzyka związanego z bezpieczeństwem, zarządzania incydentami i zarządzania zgodnością. Osoba trzecia powiadomi Interesariusza z BT o danych kontaktowych tych osób oraz o wszelkich ich zmianach.

3.33 Osoba trzecia poinformuje BT pocztą elektroniczną na adres security@bt.com lub telefonicznie pod numerem 0800 321 999 w rozsądnym terminie po uzyskaniu informacji o jakimkolwiek Incydencie mającym wpływ na usługę BT lub Informacje BT, a w każdym razie nie później niż dwadzieścia cztery (24) godziny od momentu, w którym Osoba trzecia dowie się o Incydencie.

3.34 Osoba trzecia bez nieuzasadnionej zwłoki podejmie odpowiednie i terminowe działania naprawcze w celu złagodzenia wszelkich zagrożeń i skutków związanych z incydentem, aby zmniejszyć dotkliwość i czas trwania incydentu.

3.35 W ciągu 30 dni od incydentu Osoba trzecia przekaże Interesariuszowi z BT raport dotyczący każdego incydentu mającego wpływ na usługę BT lub Informacje BT, który powinien zawierać co najmniej:

datę i godzinę, lokalizację, rodzaj incydentu, wpływ, status i wynik (w tym zalecenia dotyczące rozwiązania lub podjęte działania).

3.36 Osoba trzecia musi przeprowadzić analizę przyczyn źródłowych wszystkich incydentów bezpieczeństwa. Wyniki tej analizy powinny być eskalowane do odpowiedniego poziomu zarządzania w organizacji Osoby trzeciej.

Zarządzanie zmianą

3.37 Osoba trzecia musi zapewnić, że wszystkie zmiany IT są zatwierdzane, rejestrowane i testowane, w tym wycofywanie nieudanych zmian, przed ich wdrożeniem, aby zapobiec zakłóceniom usług lub naruszeniom bezpieczeństwa oraz że istnieje proces przeprowadzania aktualizacji awaryjnych w kontrolowany sposób.

3.38 Osoba trzecia musi zapewnić, że zmiany zostaną odzwierciedlone zarówno w środowisku produkcyjnym, jak i DR.

3.39 Osoba trzecia musi zapewnić, że konserwacja i naprawa aktywów organizacyjnych jest wykonywana i rejestrowana przy użyciu zatwierdzonych i kontrolowanych narzędzi.

3.40 Osoba trzecia musi zapewnić, że zdalna konserwacja zasobów organizacyjnych jest zatwierdzona, rejestrowana i wykonywana w sposób uniemożliwiający nieautoryzowany dostęp.

Zarządzanie ryzykiem i zagrożeniami cybernetycznymi

3.41 Osoba trzecia musi zapewnić, że istnieją bieżące ramy oceny ryzyka cyberbezpieczeństwa i zagrożeń, aby zapewnić, że profil ryzyka cyberbezpieczeństwa dla operacji, aktywów, obiektów i osób organizacji jest zrozumiały i zarządzany przez:

- Ocenę słabych punktów zasobów.
- Identyfikację zagrożeń wewnętrznych i zewnętrznych.
- Wrażliwość informacji / danych objętych zakresem.
- Ocenę potencjalnych skutków biznesowych.
- Zagrożenia, podatności, prawdopodobieństwa i skutki są wykorzystywane do określenia ryzyka.
- Zapewnienie, że ramy zarządzania ryzykiem cybernetycznym i zagrożeniami są uzgodnione na odpowiednim poziomie w organizacji.

3.42 Osoba trzecia musi zapewnić, że wszystkie ryzyka i zagrożenia zidentyfikowane w ramach oceny ryzyka i zagrożeń cyberbezpieczeństwa są traktowane priorytetowo i podejmowane są odpowiednie działania w celu złagodzenia ryzyka w odpowiednich ramach czasowych.

3.43 Osoba trzecia musi powiadomić interesariusza BT, jeśli nie jest w stanie naprawić lub ograniczyć istotnych obszarów ryzyka, które mogą mieć wpływ na świadczoną usługę.

Zarządzanie tożsamością i kontrola dostępu

3.44 Osoba trzecia musi mieć ustanowione i spójne ramy w celu zapewnienia bezpiecznego zarządzania tożsamościami i danymi uwierzytelniającymi przez upoważniony personel:

- Przyznawanie, ponowne włączanie, zmienianie i wyłączanie praw dostępu odbywa się wyłącznie na podstawie udokumentowanych i autoryzowanych zatwierdzeń.
- Upewnienie się, że nieaktywne konta są wyłączone.
- Wyłączanie kont personelu, który nie jest już zatrudniony.
- Wdrażanie procesów i narzędzi do śledzenia, kontrolowania, zapobiegania i korygowania wykorzystania, przypisywania i konfigurowania uprawnień administracyjnych na komputerach, w sieciach i aplikacjach.
- Okresowe przeglądy dostępu mają na celu zapewnienie, że dostęp jest odpowiedni do celu.
- Dostęp do kont użytkowników jest weryfikowany co najmniej raz w roku, a dostęp do kont uprzywilejowanych jest weryfikowany raz na kwartał.
- Upewnienie się, że trwałe dane uwierzytelniające i sekrety (np. w celu uzyskania dostępu przez szybę) są chronione w pamięci masowej chronionej sprzętowo i są udostępniane wyłącznie osobom odpowiedzialnym w sytuacjach awaryjnych.
- Upewnienie się, że nietrwałe dane uwierzytelniające (np. nazwa użytkownika i hasło) są przechowywane w scentralizowanej usłudze z odpowiednią kontrolą

dostępu opartą na rolach, która powinna być aktualizowana zgodnie z wszelkimi istotnymi zmianami ról i obowiązków w organizacji.

3.45 Centralne przechowywanie trwałych danych uwierzytelniających powinno być chronione sprzętowo. Na przykład na fizycznym hoście dysk może być zaszyfrowany przy użyciu modułu Trusted Platform Module (TPM). W przypadku, gdy maszyna wirtualna (VM) jest używana do świadczenia usługi centralnej pamięci masowej, ta maszyna wirtualna i zawarte w niej dane muszą być również zaszyfrowane; VM musi używać bezpiecznego rozruchu i być skonfigurowana tak, aby zapewnić możliwość uruchomienia tylko w odpowiednim środowisku. Osoba trzecia musi zapewnić, że zdalny dostęp jest zarządzany w taki sposób, że tylko zatwierdzone osoby mogą łączyć się zdalnie z Systemami Osoby trzeciej oraz że połączenia są bezpieczne i zapobiegają wyciekowi danych, a także że istnieje odpowiednia kontrola dostępu, taka jak uwierzytelnianie wieloskładnikowe.

Uwierzytelnianie dwuskładnikowe powinno być realizowane za pomocą identyfikatora użytkownika, hasła i jednej z poniższych metod:

- Generator haseł jednorazowych: wymaga podania kodu PIN/hasła użytkownika, aby wyświetlić hasło jednorazowe.
- Karta inteligentna z chipem zgodnym z normą ISO 7816 oraz powiązanym czytnikiem kart i oprogramowaniem. Bezstykowe karty inteligentne nie są dozwolone.
- Uwierzytelnianie oparte na certyfikatach wydane zgodnie z polityką certyfikatów Infosec osoby trzeciej.

Aby uniknąć wątpliwości, jeśli uprzywilejowany dostęp do pomocy technicznej jest zapewniany za pośrednictwem zdalnego dostępu, musi on odbywać się za pośrednictwem bezpiecznego połączenia i wykorzystywać uwierzytelnianie dwuskładnikowe.

3.46 Osoba trzecia musi zapewnić, że uprawnienia dostępu i autoryzacje dla wszystkich systemów (w tym narzędzi, aplikacji, baz danych, systemów operacyjnych, sprzętu itp.) są zarządzane z uwzględnieniem zasad najmniejszych uprawnień i rozdziału obowiązków.

3.47 Osoba trzecia musi zapewnić, że każda transakcja może być przypisana do unikalnej, możliwej do zidentyfikowania osoby, a jeśli istnieją jakiekolwiek wspólne dane uwierzytelniające, że istnieją odpowiednie kontrole kompensacyjne (w tym procedury „break-glass”). Współdzielone dane uwierzytelniające dla uprzywilejowanego dostępu są niedozwolone.

3.48 Osoba trzecia musi zapewnić, że całe uwierzytelnianie jest zarządzane współmiernie do ryzyka transakcji, tj. odpowiednia długość i złożoność hasła, częstotliwość zmian haseł, uwierzytelnianie wieloskładnikowe, bezpieczne zarządzanie danymi uwierzytelniającymi hasła lub inne środki kontroli. Uprzywilejowany dostęp musi odbywać się za pośrednictwem kont zabezpieczonych uwierzytelnianiem wieloskładnikowym. Uprzywilejowane konta użytkowników typu „break-glass” muszą mieć silne poświadczenia unikalne dla każdego punktu dostępu do sprzętu sieciowego.

3.49 Muszą istnieć odpowiednie mechanizmy kontrolne do obsługi nieudanych uwierzytelnień, w tym powiadomienia ekranowe, rejestrowanie niepowodzeń i blokowanie użytkownika.

3.50 Należy wdrożyć procesy i mechanizmy kontroli w celu zarządzania kontami gości i usług oraz ich autoryzacji.

Klasyfikacja i ochrona danych

3.51 Osoba trzecia musi posiadać ustalone i spójne ramy / schemat klasyfikacji, etykietowania i postępowania z informacjami (dostosowane do Dobrych praktyk branżowych / wymogów BT), które zawierają następujące elementy:

- Wytyczne dotyczące przetwarzania informacji.
- Informacje są chronione zgodnie z przypisanym im poziomem klasyfikacji.
- Zapewnienie, aby wszyscy pracownicy byli świadomi, że informacje BT nie będą wykorzystywane do celów innych niż te, dla których zostały dostarczone.

Zapobieganie wyciekom danych

3.52 Osoba trzecia musi mieć ustanowione i spójne ramy w celu zapewnienia ochrony przed niewłaściwym wyciekiem danych, zapewniając ochronę obejmującą (ale nie ograniczającą się do) następujące wektory:

- Poczta e-mail, Internet / brama internetowa (w tym pamięć masowa online i poczta internetowa), USB, optyczne i inne formy portów / przenośnych pamięci masowych itp., komputery mobilne i BYOD, usługi zdalnego dostępu, mechanizmy udostępniania plików i media społecznościowe.
- Nieautoryzowane urządzenia nie mogą być podłączane do sieci (ani do sieci korporacyjnej dostawcy, ani do systemów/sieci BT) ani wykorzystywane do uzyskiwania dostępu do informacji niepublicznych.

Zarządzanie lukami w zabezpieczeniach.

3.53 Osoba trzecia musi posiadać ustanowione i spójne ramy zarządzania lukami w zabezpieczeniach, które obejmują następujące elementy:

- Polityki i procedury dotyczące procesów.
- Zdefiniowane role i obowiązki.
- Odpowiednie narzędzia, takie jak systemy wykrywania włamań i systemy skanowania podatności.

3.54 Ramy zarządzania lukami w zabezpieczeniach osoby trzeciej muszą zapewniać rutynowe monitorowanie następujących elementów w celu wykrywania potencjalnych zdarzeń związanych z cyberbezpieczeństwem:

- Kluczowe systemy i zasoby.
- Nieautoryzowane połączenia.
- Nieautoryzowane oprogramowanie/aplikacje.
- Aktywność w sieci.

3.55 Ramy zarządzania lukami w zabezpieczeniach osoby trzeciej muszą zapewniać, że

- Istnieją procesy ustanowione w celu odbierania, analizowania i reagowania na luki w zabezpieczeniach ujawnione organizacji ze źródeł wewnętrznych i zewnętrznych (np. testy wewnętrzne, biuletyny bezpieczeństwa lub badacze bezpieczeństwa).
- Dozwolone są tylko autoryzowane narzędzia, technologie i użytkownicy.
- Zidentyfikowane słabe punkty są łagodzone lub dokumentowane jako zaakceptowane ryzyko.

Ciągłe rejestrowanie i monitorowanie bezpieczeństwa.

3.56 Osoba trzecia musi zapewnić, że istnieją ustalone i spójne ramy audytu i zarządzania dziennikami, które zapewniają, że kluczowe systemy, w tym aplikacje, są ustawione na rejestrowanie kluczowych zdarzeń (w tym tych związanych z uprzywilejowanym dostępem i aktywnością personelu), a takie dzienniki są przechowywane przez okres co najmniej 13 miesięcy. Dzienniki dla urządzeń sieciowych w krytycznych funkcjach bezpieczeństwa muszą być w pełni rejestrowane i udostępniane do audytu przez 13 miesięcy.

Jako minimum, Osoba trzecia musi zapewnić, że dzienniki dotyczą następujących zdarzeń:

- Uruchamianie i wyłączanie systemu.
- Udane i nieudane uwierzytelnianie
- Logowanie i wylogowanie z systemu
- Tworzenie, modyfikowanie i usuwanie kont
- Zmiana poświadczeń
- Eskalacja uprawnień
- Blokada konta
- Dołączanie i usuwanie sprzętu
- Alerty i komunikaty o błędach dotyczące zarządzania systemem i siecią
- Zmiany administratora zdarzeń bezpieczeństwa, w tym zarządzanie grupami i zmiany zasad bezpieczeństwa
- Punkty rozpoczęcia i zakończenia rejestrowanego procesu
- Rejestrowanie zdarzeń aktywacji lub dezaktywacji
- Zmiany typu rejestrowanych zdarzeń zgodnie z wymaganiami ścieżki audytu (na przykład parametry rozruchu i wszelkie ich zmiany).
- Modyfikacja dziennika (lub próba modyfikacji)
- Jakakolwiek forma dostępu do płaszczyzny zarządzania systemami używanymi w związku z brytyjską publiczną siecią lub usługą łączności elektronicznej

Jako minimum, osoba trzecia musi zapewnić, że następujące parametry dziennika są rejestrowane dla każdego zdarzenia:

- Tożsamość składnika aktywów, którego dotyczy zdarzenie
- Rodzaj zdarzenia
- Data i godzina zdarzenia

- Wskazanie sukcesu/porażki zdarzenia
- Identyfikator użytkownika konta
- Identyfikacja źródła zdarzenia, taka jak lokalizacja użytkownika/systemu, adresy IP, identyfikator terminala, identyfikator terminala lub inne środki identyfikacji

3.57 Struktura audytu, rejestrowania i monitorowania osoby trzeciej musi obejmować następujące elementy:

- Dzienniki zdarzeń generują alerty w czasie rzeczywistym lub zbliżonym do rzeczywistego w celu zidentyfikowania nieautoryzowanej aktywności.
- Zdarzenia i alerty są monitorowane przez niezależną funkcję w sposób ciągły i są badane, segregowane i przypisywany jest im poziom ważności
- Sprawdzone alerty uruchamiają procesy zarządzania incydentami bezpieczeństwa w oparciu o ustalone przypadki użycia monitorowania ochronnego i podręczniki odtwarzania zgodnie z umowami o poziomie usług i dotkliwością.
- Dzienniki są traktowane jako informacje o klauzuli co najmniej „poufne" i są chronione przed manipulacją, nieautoryzowanym dostępem i utratą.
- Rejestrowanie i monitorowanie aktywności jest zsynchronizowane z zatwierdzonym źródłem czasu NTP
- Ustanowiono procesy w celu zidentyfikowania i skonfigurowania dodatkowych przypadków użycia monitorowania ochronnego i powiązanych dzienników zdarzeń, korelacji i alertów niezbędnych do przeciwdziałania istniejącym lub pojawiającym się istotnym zagrożeniom i ryzyku.

4. Bezpieczeństwo personelu Osoby trzeciej

4.1 Osoba trzecia zapewni zawarcie umów o zachowaniu poufności przez cały Personel Osoby trzeciej przed rozpoczęciem przez Personel Osoby trzeciej pracy w budynkach BT lub w Systemach BT lub przed uzyskaniem dostępu do Informacji BT. Umowy o zachowaniu poufności muszą być przechowywane przez Osobę trzecią, a dowody muszą być udostępniane do celów audytu przez BT.

4.2 Osoba trzecia będzie zajmować się naruszeniami kontroli i standardów bezpieczeństwa Osoby trzeciej i BT w drodze formalnych procesów, w tym działań dyscyplinarnych, które mogą obejmować usunięcie danej osoby z firmy:

- posiadanie dostępu do systemów BT lub informacji BT; lub
- wykonywanie prac związanych ze świadczeniem Usługi.

Ponadto Osoba trzecia zapewni wdrożenie odpowiednich procesów w celu zagwarantowania, że Personel Osoby trzeciej, który został w ten sposób usunięty, nie uzyska następnie dostępu do Systemów BT, Informacji BT ani nie zostanie dopuszczony do pracy w związku ze świadczeniem Usługi.

4.3 Osoba trzecia będzie, w zakresie dopuszczalnym przez prawo, utrzymywać poufny system, z którego Personel Osoby trzeciej będzie mógł korzystać w celu anonimowego zgłaszania przypadków, w których zostanie poinstruowany do działania w sposób

niezgodny lub naruszający niniejsze Wymogi bezpieczeństwa. Odpowiednie raporty należy zgłaszać BT.

4.4 Gdy Personel Osoby trzeciej nie jest już przypisany do Usługi, według uznania BT, wszelkie aktywa rzeczowe BT lub Informacje BT będące w posiadaniu Personelu Osoby trzeciej zostaną: przekazane z powrotem odpowiedniemu zespołowi operacyjnemu BT lub bezpiecznie zniszczone zgodnie ze środkami kontroli bezpieczeństwa 3.22 i 3.23.

4.5 Osoba trzecia musi mieć ustalone i spójne ramy dotyczące dopuszczalnego korzystania z osobistych i korporacyjnych mediów społecznościowych, w tym zapewnienia, aby personel:

- nie publikował żadnych oszczerczych, obscenicznych lub obraźliwych treści na temat organizacji, jej klientów lub odbiorców.
- nie używał logo organizacji lub klienta bez uprzedniej zgody.
- nie ujawniał niepublicznych informacji o organizacji lub kliencie bez uprzedniej zgody.
- nie publikował opinii na temat organizacji, jej klientów lub klientów, które mogłyby być interpretowane jako oficjalny komentarz organizacji lub jej klientów.
- nie ujawniał żadnych informacji BT oznaczonych jako „Ogólne", „Poufne" lub „Wysoce poufne".

4.6 Osoba trzecia musi zapewnić, że cały Personel Osoby trzeciej pozostający pod jej kontrolą przejdzie obowiązkowe szkolenie w zakresie bezpieczeństwa informacji, które obejmuje najlepsze praktyki w zakresie cyberbezpieczeństwa i ochrony danych osobowych w ciągu jednego miesiąca od rozpoczęcia pracy i będzie odświeżane co najmniej raz w roku, w tym w stosownych przypadkach:

- użytkownicy uprzywilejowani
- interesariusze zewnętrzni (np. podwykonawcy, klienci, partnerzy)
- kierownictwo wyższego szczebla
- personel ds. bezpieczeństwa fizycznego i cyberbezpieczeństwa

4.7 Osoba trzecia musi zapewnić komponent testowy w celu sprawdzenia, czy użytkownik rozumie szkolenie i świadomość.

5. Audyt i przegląd bezpieczeństwa

5.1 Bez uszczerbku dla jakiegokolwiek innego prawa do audytu, jakie może przysługiwać BT, w celu oceny zgodności Osoby trzeciej z mechanizmami kontroli bezpieczeństwa określonymi w niniejszej polityce dotyczącej wymogów bezpieczeństwa, Osoba trzecia zapewni BT lub jej przedstawicielom dostęp i pomoc w zakresie niezbędnym i odpowiednim do umożliwienia przeprowadzenia przeglądów bezpieczeństwa opartych na dokumentacji lub audytów na miejscu. Osoba trzecia zostanie powiadomiona o rutynowym audycie na miejscu z wyprzedzeniem co najmniej 30 dni roboczych.

Zakres audytu będzie obejmował przegląd wszelkich aspektów polityk, procesów i systemów Osoby trzeciej (z zastrzeżeniem, że Osoba trzecia będzie chronić poufność wszelkich informacji niezwiązanych ze świadczeniem Usługi na rzecz BT), które są istotne dla świadczonej Usługi.

5.2 Osoba trzecia będzie współpracować z BT w celu wdrożenia uzgodnionych zaleceń i przeprowadzenia wszelkich działań naprawczych określonych jako konieczne w wyniku przeglądu bezpieczeństwa opartego na dokumentach lub audytu na miejscu w ciągu 30 dni od powiadomienia przez BT o poważnej niezgodności, 90 dni od powiadomienia przez BT o drobnej niezgodności lub w okresie uzgodnionym między stronami na koszt Osoby trzeciej.

6. Prawo do inspekcji

6.1 Osoba trzecia musi zezwolić BT na przeprowadzenie inspekcji środowiska kontroli, w którym usługi są opracowywane, wytwarzane lub świadczone, w celu przeprowadzenia testów zgodności i/lub ocen bezpieczeństwa na uzasadnione żądanie (lub niezwłocznie po wystąpieniu incydentu).

6.2 Osoba trzecia jest odpowiedzialna za koszty usunięcia wszelkich słabych punktów bezpieczeństwa zidentyfikowanych przez BT w terminie uzgodnionym przez obie Strony.

6.3 W przypadku poważnego incydentu Osoba trzecia będzie w pełni współpracować z BT we wszelkich dochodzeniach prowadzonych przez BT, organ regulacyjny i/lub organ ścigania, zapewniając dostęp i pomoc w zakresie niezbędnym i właściwym do zbadania incydentu. BT może zażądać od Osoby trzeciej poddania kwarantannie w celu oceny wszelkich istotnych aktywów należących do Osoby trzeciej, aby wspomóc dochodzenie, a Osoba trzecia nie będzie bezzasadnie odmawiać ani opóźniać takiego żądania.

7. Certyfikaty bezpieczeństwa

7.1 Systemy, usługi, powiązane usługi, procesy i fizyczne lokalizacje Osoby trzeciej muszą być zgodne z normą ISO/IEC 27001 (lub certyfikatami, które wykazują równoważne kontrole, poparte raportem niezależnego audytora) i wszelkimi zmienionymi lub przyszłymi wersjami wydanej normy. Zgodność ta musi być zapewniona poprzez certyfikację ISMS Osoby trzeciej przez brytyjską służbę akredytacyjną (UKAS) lub międzynarodową równoważną zatwierdzoną jednostkę certyfikującą, której zakres i oświadczenie o stosowalności obejmuje usługi świadczone w lokalizacjach, z których będą świadczone.

7.2 Osoba trzecia musi przedłożyć ważny certyfikat na początku obowiązywania umowy i przy kolejnych ponownych certyfikacjach.

7.3 W przypadku zmiany zakresu certyfikatu lub oświadczenia o stosowalności w okresie obowiązywania umowy w zakresie, w jakim nie obejmuje on już wszystkich usług świadczonych w lokalizacjach, z których są one świadczone, Osoba trzecia musi powiadomić o tym BT w rozsądnym terminie. Osoba trzecia musi poinformować BT w ciągu 2 dni roboczych o wszelkich poważnych niezgodnościach zidentyfikowanych przez jednostkę certyfikującą lub Osobę trzecią, które stwarzają ryzyko dla świadczonych usług.

8. Bezpieczeństwo fizyczne - lokalizacja BT

8.1 Osoba trzecia będzie przestrzegać wszystkich stosownych instrukcji przekazanych jej w odniesieniu do dostępu do obiektów BT i systemów wejściowych do budynków. Cały Personel Osoby trzeciej pracujący na terenie BT musi posiadać i umieszczać w widocznym miejscu kartę identyfikacyjną Osoby trzeciej lub firmy BT, która musi zawierać zdjęcie umieszczone na karcie, które jest wyraźnym i prawdziwym wizerunkiem Personelu Osoby trzeciej.

8.2 BT może również zapewnić Personelowi Osoby trzeciej elektroniczną kartę dostępu i/lub kartę gościa o ograniczonym czasie ważności, które będą używane zgodnie z lokalnymi instrukcjami wydawania i unieważniania kart.

8.3 Osoba trzecia jest odpowiedzialna za powiadomienie BT w ciągu 24 godzin, gdy osoba będąca Osobą trzecią nie potrzebuje już dostępu do budynków BT i/lub dostępu do systemów wejściowych BT.

8.4 Tylko zatwierdzone serwery BT Build, komputery BT Webtop i zaufane urządzenia końcowe mogą bezpośrednio łączyć się (podłączać do portu LAN lub połączenia bezprzewodowego) z domenami BT. Osobom trzecim nie wolno bez uprzedniej pisemnej zgody BT podłączać do żadnej domeny BT żadnego sprzętu niezatwierdzonego przez BT.

8.5 Ochrona fizyczna i wytyczne dotyczące pracy w obiektach BT będą przestrzegane i będą obejmować między innymi eskortowanie personelu osób trzecich oraz przyjęcie odpowiednich praktyk pracy w zabezpieczonych obszarach.

8.6 W przypadku, gdy Osoba trzecia jest upoważniona do zapewnienia swojemu Personelowi Osoby trzeciej nieobsługiwanego dostępu do obszarów należących do BT, upoważniony sygnatariusz Osoby trzeciej i Personel Osoby trzeciej muszą przestrzegać wytycznych zawartych w dokumencie Dostęp dostawców do lokalizacji BT – Obowiązkowy przewodnik dotyczący bezpieczeństwa Sprzedaż na rzecz BT.

9. Bezpieczeństwo fizyczne - lokalizacja osoby trzeciej

9.1 Osoba trzecia musi dysponować procesem fizycznego dostępu, który obejmuje metody dostępu i autoryzację do pomieszczeń Osoby trzeciej (lokalizacji, budynków lub obszarów wewnętrznych), w których świadczone są usługi lub w których przechowywane lub przetwarzane są Informacje BT. Metoda dostępu powinna obejmować co najmniej 1 z poniższych:

- Autoryzowana karta identyfikacyjna Osoby trzeciej ze zdjęciem umieszczonym na karcie, które jest wyraźne i stanowi wierne odwzorowanie danej osoby.
- Autoryzowana elektroniczna karta dostępu umożliwiająca dostęp do odpowiednich obszarów obiektu.
- Dostęp bezpieczeństwa do klawiatury, który musi obejmować procesy: autoryzacji, rozpowszechniania zmian kodu (które muszą następować co najmniej raz w miesiącu) oraz doraźnych zmian kodu.
- Rozpoznawanie biometryczne.

9.2 Osoba trzecia musi posiadać procesy i procedury kontroli i monitorowania gości i innych osób zewnętrznych, w tym personelu z fizycznym dostępem do zabezpieczonych

obszarów lub w celu konserwacji kontroli środowiskowej, konserwacji alarmów i czyszczenia.

9.3 Bezpieczne obszary w obiektach Osób trzecich wykorzystywane do świadczenia usługi (np. pomieszczenia komunikacji sieciowej) muszą być oddzielone od obszarów ogólnego dostępu i chronione przez odpowiednie kontrole wejścia w celu zapewnienia, że tylko upoważnione osoby mają do nich dostęp. Dostęp do tych obszarów musi być regularnie kontrolowany, a ocena ponownej autoryzacji praw dostępu do tych obszarów musi być przeprowadzana co najmniej raz w roku.

9.4 Osoba trzecia musi posiadać systemy bezpieczeństwa CCTV w miejscach, w których przechowywane lub przetwarzane są Informacje BT. Nagrania i rejestratory muszą być bezpiecznie zlokalizowane, aby zapobiec modyfikacji, usunięciu lub „przypadkowemu" przeglądaniu powiązanych ekranów CCTV, a dostęp do nagrań musi być kontrolowany i ograniczony wyłącznie do upoważnionych osób. Nagrania CCTV muszą być przechowywane przez co najmniej 20 dni.

9.5 Osoba trzecia musi wdrożyć odpowiednie środki w celu zapewnienia bezpieczeństwa fizycznego w odniesieniu do następujących elementów:

- Środki zapobiegania pożarom, w tym między innymi alarmy, sprzęt do wykrywania i gaszenia pożarów.
- Warunki klimatyczne, z uwzględnieniem temperatury, wilgotności i elektryczności statycznej oraz powiązanego zarządzania, monitorowania i reagowania na ekstremalne warunki (takie jak automatyczne wyłączanie, alarmy).
- Urządzenia sterujące, w tym między innymi klimatyzacja i wykrywanie wody.
- Zapobieganie uszkodzeniom spowodowanym przez wodę, lokalizacja zbiorników na wodę, rur itp. na terenie obiektu.

9.6 Osoba trzecia musi zapewnić, że fizyczny dostęp do obszarów, w których przechowywane są Informacje BT, odbywa się za pomocą kart inteligentnych lub zbliżeniowych (lub równoważnych lub lepszych systemów bezpieczeństwa), a Osoba trzecia musi przeprowadzać comiesięczne kontrole w celu zapewnienia, że tylko odpowiednie osoby mają taki dostęp.

9.7 Osoba trzecia musi zapewnić, że fotografowanie i/lub przechwytywanie obrazów jakichkolwiek Informacji BT jest zabronione. W przypadku, gdy istnieje potrzeba biznesowa przechwytywania takich obrazów, należy uzyskać pisemne potwierdzenie od Interesariusza BT.

10. Zapewnienie środowiska hostingowego dla sprzętu BT

10.1 Osoba trzecia musi, w przypadku gdy zapewnia bezpieczny obszar dostępu w swoich obiektach na potrzeby hostingu sprzętu BT lub klientów BT:

- Dostarczyć BT plan piętra przydzielonej przestrzeni w zabezpieczonym obszarze lokalu.
- Upewnić się, że szafki BT i klienta BT w obiektach są zamknięte i mają do nich dostęp wyłącznie upoważnieni pracownicy BT, zatwierdzeni przedstawiciele BT i odpowiedni personel Osoby trzeciej.
- Wdrożyć bezpieczny proces zarządzania kluczami.

10.2 BT dostarczy Osobie trzeciej:

- Rejestr fizycznych aktywów BT i/lub klienta BT przechowywanych w siedzibie Osoby trzeciej.
- Szczegóły dotyczące pracowników, podwykonawców i agentów BT, którzy potrzebują dostępu do obiektów Osoby trzeciej (na bieżąco).

11. Bezpieczne tworzenie oprogramowania

11.1 Osoba trzecia musi zapewnić, że środowiska produkcyjne i nieprodukcyjne są odpowiednio kontrolowane poprzez zapewnienie następujących elementów:

- Segregacja środowisk produkcyjnych i nieprodukcyjnych z podziałem obowiązków.
- Żadne rzeczywiste dane nie mogą być wykorzystywane w testach, chyba że zostanie wydana wcześniejsza zgoda właścicieli danych i będą stosowane kontrole współmierne do środowiska produkcyjnego.
- Segregacja obowiązków między rozwojem produkcyjnym i nieprodukcyjnym.

11.2 Osoba trzecia musi posiadać ustanowione i spójne ramy rozwoju systemów w celu zapobiegania lukom w zabezpieczeniach i naruszeniom cyberbezpieczeństwa, które obejmują następujące elementy:

- Systemy są rozwijane zgodnie z najlepszymi praktykami bezpiecznego rozwoju (np. OWASP).
- Kod jest bezpiecznie przechowywany i podlega kontroli jakości.
- Kod jest odpowiednio chroniony przed nieautoryzowanymi modyfikacjami po zatwierdzeniu testów i dostarczeniu do produkcji.

12. Umowa powiernicza

12.1 W przypadku, gdy wymagana jest umowa powiernicza w celu ochrony wszystkich stron zarówno dla osoby pierwszej, jak osoby trzeciej (tj. dla własności intelektualnej / kodu źródłowego itp.), Osoba trzecia musi mieć spójne i ustalone ramy, które obejmują następujące elementy:

- Zawarcie umowy powierniczej z niezależnym, neutralnym i renomowanym agentem powierniczym.
- Dostarczanie i bieżąca aktualizacja kodu źródłowego i innych materiałów agentowi Escrow w celu zapewnienia aktualności wymaganych informacji.
- Bezpieczne przechowywanie kodu źródłowego i innych materiałów do czasu spełnienia warunków zwolnienia.
- Odpowiednie warunki zwolnienia.
- Bieżące aktualizacje, odpowiednie płatności i przeglądy umowy Escrow.

13. Dostęp do systemów BT

13.1 Osoba trzecia będzie przestrzegać wszystkich przekazanych jej stosownych instrukcji dotyczących dostępu do Systemów BT i korzystania z nich.

13.2 Osoba trzecia jest odpowiedzialna za powiadomienie BT w ciągu 24 godzin, gdy osoba będąca Osobą trzecią nie potrzebuje już dostępu.

13.3 Osoba trzecia zapewni, że identyfikacja użytkownika, hasła, kody PIN, tokeny i dostęp do konferencji są przeznaczone dla indywidualnego Personelu Osoby trzeciej i nie są udostępniane. Dane muszą być przechowywane bezpiecznie i oddzielnie od urządzenia używanego do uzyskania dostępu. Jeśli hasło jest znane innej osobie, należy je natychmiast zmienić.

Łączność między systemami

13.4 Łączenie między domenami z systemami BT jest niedozwolone, chyba że zostało wyraźnie zatwierdzone i autoryzowane przez BT.

13.5 Osoba trzecia musi dołożyć wszelkich uzasadnionych starań, aby zapewnić, że do Systemów BT nie zostanie wprowadzone złośliwe oprogramowanie (w rozumieniu powszechnie przyjętym w branży komputerowej).

13.6 Tam, gdzie istnieje łączność między systemami osoby trzeciej i BT, łączność będzie odbywać się za pośrednictwem bezpiecznych łączy z danymi chronionymi za pomocą szyfrowania zgodnego z kontrolami kryptograficznymi w punktach 14.9, 14.10, 14.11, 14.12 i 14.13.

13.7 Osoba trzecia zapewni, że wykorzystywane systemy i infrastruktura są zawarte w dedykowanej sieci logicznej. Sieć ta musi składać się wyłącznie z systemów dedykowanych do bezpiecznego przetwarzania danych klientów.

14. Systemy osób trzecich przechowujące informacje BT

14.1 Osoba trzecia musi zapewnić, że najnowsze poprawki zabezpieczeń są stosowane do systemów/ zasobów/sieci/aplikacji, zapewniając, że:

- Osoba trzecia wdraża poprawki tak szybko, jak to możliwe, i dokłada wszelkich starań, aby wdrożyć je w następujących ramach czasowych po wydaniu poprawki:

	Aktywnie wykorzystywane na wolności	**Wysoki wskaźnik EPSS** Luki w zabezpieczeniach CVSS: > 8.0 (wysoki + krytyczny) EPSS: >= 70% (Wektor ataku sieciowego – patrz część z definicjami)	**Niższy wskaźnik EPSS** Luki w zabezpieczeniach CVSS: > 8.0 (wysoki + krytyczny) EPSS: < 70% (Wektor ataku sieciowego – patrz część z definicjami)	**Inne** (wektor ataku niesieciowego)
Interfejs wyeksponowany na zewnątrz	7 dni	14 dni	30 dni	90 dni
Interfejs wyeksponowany do wewnątrz	7 dni	14 dni	30 dni	90 dni/BAU

- Osoba trzecia wykorzystuje poprawki uzyskane od: dostawców bezpośrednio dla systemów zastrzeżonych i poprawek, które są (i) podpisane cyfrowo lub (ii) zweryfikowane za pomocą skrótu dostawcy (nie wolno używać skrótów MD5) dla pakietu aktualizacji, tak aby poprawka mogła zostać zidentyfikowana jako pochodząca od renomowanej społeczności wsparcia dla oprogramowania typu open source.
- Osoba trzecia testuje wszystkie poprawki na systemach, które dokładnie reprezentują konfigurację docelowych systemów produkcyjnych przed wdrożeniem poprawki do systemów produkcyjnych, a prawidłowe działanie poprawionej usługi jest weryfikowane po każdej czynności związanej z łataniem.
- Monitorowanie wszystkich odpowiednich dostawców i innych istotnych źródeł informacji pod kątem alertów o lukach w zabezpieczeniach.
- Jeśli system nie może zostać załatany, należy wdrożyć odpowiednie środki zaradcze.
- Osoba trzecia będzie instalować krytyczne poprawki zabezpieczeń oddzielnie od wydań funkcji, aby zmaksymalizować szybkość, z jaką można wdrożyć poprawkę, i w miarę możliwości będzie nadawać priorytet krytycznym poprawkom zabezpieczeń nad aktualizacjami funkcji.

14.2 Osoba trzecia musi zapewnić, że co najmniej raz w roku zlecana jest niezależna ocena bezpieczeństwa IT / test penetracyjny zatwierdzony przez BT Security w odniesieniu do

infrastruktury IT Osoby trzeciej i aplikacji wykorzystywanych do świadczenia usług, w tym lokalizacji Disaster Recovery, w celu zidentyfikowania luk w zabezpieczeniach, które mogą zostać wykorzystane do naruszenia danych / usług oraz w celu zapobiegania wszelkim naruszeniom bezpieczeństwa poprzez ataki cybernetyczne. Osoba trzecia musi na uzasadniony wniosek zezwolić BT na dostęp do raportów z testów penetracyjnych dotyczących świadczonych usług.

14.3 Osoba trzecia musi zapewnić bezpieczną kontrolę dostępu do portów diagnostycznych i zarządzających, a także narzędzi diagnostycznych.

14.4 Osoba trzecia musi zapewnić, że dostęp do narzędzi audytowych jest ograniczony do odpowiedniego personelu dostawcy, a ich użycie jest monitorowane.

14.5 Osoba trzecia musi zapewnić, że żadne serwery używane do świadczenia usługi nie są wdrażane w niezaufanych sieciach (sieciach poza obszarem bezpieczeństwa Osoby trzeciej, które są poza jej kontrolą administracyjną, np. w Internecie) bez odpowiedniej kontroli bezpieczeństwa.

Zarządzanie aktywami

14.6 Osoba trzecia musi prowadzić dokładną i aktualną inwentaryzację zasobów informacyjnych wszystkich zasobów technologicznych, które mogą przechowywać lub przetwarzać informacje, tak aby tylko autoryzowane urządzenia miały dostęp, a nieautoryzowane i niezarządzane urządzenia zostały znalezione i uniemożliwiono im uzyskanie dostępu. Inwentaryzacja ta powinna obejmować wszystkie zasoby sprzętowe, niezależnie od tego, czy są one podłączone do sieci organizacji. W stosownych przypadkach inwentaryzacją należy objąć wszelkie urządzenia BT hostowane w obiektach osób trzecich.

14.7 Osoba trzecia musi zapewnić, że inwentaryzacja zasobów informacyjnych obejmuje następujące elementy zinwentaryzowane lub skatalogowane:

- Urządzenia i systemy fizyczne, platformy programowe i aplikacje, zewnętrzne systemy informatyczne.
- Zasoby (np. sprzęt, urządzenia, dane, czas i oprogramowanie) są traktowane priorytetowo na podstawie ich klasyfikacji, krytyczności i wartości biznesowej.
- Przepływy danych organizacyjnych i komunikacyjnych, w tym przepływy zewnętrzne / osób trzecich.
- Ręczne procesy obsługujące dane BT lub dane klientów BT.

14.8 Osoba trzecia musi prowadzić dokładną i aktualną inwentaryzację zasobów oprogramowania dla całego oprogramowania w sieci, tak aby tylko autoryzowane oprogramowanie było instalowane i mogło być uruchamiane, a nieautoryzowane i niezarządzane oprogramowanie było wykrywane i uniemożliwiane jego instalowanie lub uruchamianie.

Kryptografia

14.9 Osoba trzecia musi zapewnić, że Informacje BT sklasyfikowane jako Poufne lub wyższe są odpowiednio szyfrowane (w transporcie i w spoczynku). Wszystkie szyfrowania muszą być realizowane przy użyciu silnych, nowoczesnych algorytmów kryptograficznych i szyfrów wykorzystujących solidne mechanizmy ochrony

integralności oraz zgodnie ze standardami branżowymi dotyczącymi bezpiecznego negocjowania kluczy i protokołów oraz zarządzania kluczami. W przypadku danych w tranzycie następujące opcje TLS są niedozwolone: TLS w. 1.0, TLS w. 1.1 i SSL (dowolna wersja). Następujące opcje SSH (SFTP) są niedozwolone: SSH w. 1. Następujące opcje IPSec są niedozwolone: IKE w wersji 1.

14.10 Klucze kryptograficzne muszą spełniać lub przekraczać następujące minimalne długości:

- Klucze symetryczne (np. AES) muszą mieć długość klucza co najmniej 256 bitów.
- Klucze asymetryczne (np. RSA) muszą mieć długość klucza co najmniej 3072 bitów.
- Klucze z krzywą eliptyczną muszą mieć długość klucza wynoszącą co najmniej 384 bity.

14.11 Jeśli NIST ogłosi, że algorytm kryptograficzny nie jest już bezpieczny, nie wolno go używać w nowych wdrożeniach. Istniejące wdrożenia muszą dokonać przeglądu dalszego korzystania z przestarzałych algorytmów kryptograficznych i dostarczyć plan migracji w celu odejścia od przestarzałych algorytmów kryptograficznych na rzecz bezpieczniejszej alternatywy.

14.12 W przypadku szyfrowania symetrycznego niedozwolone są następujące algorytmy: 3DES-168 (chyba że jest to wymagane przez międzynarodowy standard), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed i ARIA.

14.13 „Salted hashes” muszą być używane do ochrony danych w pamięci masowej, np. haseł. Hashowanie może być również używane do anonimizacji danych przed ich przetworzeniem, na przykład numerów MSISDN lub płatności. Następujące algorytmy haszujące są niedozwolone: MD2, MD4, MD5 i SHA-1.

Konfiguracja systemu

14.14 Osoba trzecia musi mieć ustalone i spójne ramy w celu zapewnienia, że systemy są odpowiednio skonfigurowane, w tym następujące elementy:

- Systemy, urządzenia sieciowe są skonfigurowane tak, aby działały zgodnie z zasadami bezpieczeństwa (np. koncepcja najmniejszej funkcjonalności i brak nieautoryzowanego oprogramowania).
- Zapewnienie, że urządzenia wskazują prawidłową i spójną godzinę.
- Systemy są wolne od złośliwego oprogramowania.
- Prowadzone są odpowiednie kontrole i monitorowanie w celu zapewnienia integralności instalacji/urządzeń.

Ochrona przed złośliwym oprogramowaniem

14.15 Osoba trzecia musi zapewnić, że najbardziej aktualna ochrona przed złośliwym oprogramowaniem jest stosowana do wszystkich odpowiednich zasobów IT, aby zapobiec zakłóceniom usług lub naruszeniom bezpieczeństwa oraz zapewnić wdrożenie odpowiednich procedur uświadamiania użytkowników.

Ochrona przed złośliwym oprogramowaniem obejmuje wykrywanie (między innymi) oprogramowania ransomware, nieautoryzowanego kodu mobilnego, wirusów, oprogramowania szpiegującego, oprogramowania rejestrującego klucze, botnetów, robaków, trojanów itp.

Łagodzenie skutków odmowy usługi.

14.16 Osoba trzecia musi zapewnić ochronę kluczowych systemów przed atakami typu Denial of Service (DoS) i Distributed Denial of Service (DDoS).

15. Zewnętrzny hosting informacji BT

15.1 Oprócz środków kontroli opisanych w punkcie 14. Systemy osób trzecich przechowujące Informacje BT, w przypadku gdy osoba trzecia hostuje Informacje BT w centrum danych lub rozwiązaniu chmurowym, obiekty muszą posiadać ważny certyfikat ISO/IEC 27001 w zakresie zarządzania bezpieczeństwem (lub certyfikaty wykazujące równoważne kontrole, poparte raportem niezależnego audytora).

16. Bezpieczeństwo sieci - sieć własna BT

W przypadku, gdy Osoba trzecia będzie instalować sprzęt, konfigurować, utrzymywać, zarządzać, naprawiać lub monitorować własną sieć BT, zastosowanie będą miały następujące mechanizmy kontrolne:

16.1 Na żądanie Osoba trzecia przekaże BT imiona i nazwiska, adresy i inne dane, których BT może w uzasadniony sposób zażądać, dotyczące wszystkich członków Personelu Osoby trzeciej, którzy:

- będą od czasu do czasu bezpośrednio zaangażowani we wdrażanie, utrzymanie i/lub zarządzanie Usługami, zanim zostaną odpowiednio zaangażowani.
- będzie współpracować z BT w związku z dyskusją na temat zidentyfikowanych przez BT i/lub osobę trzecią luk w zabezpieczeniach Usług.

16.2 W związku z działalnością pomocniczą prowadzoną w Wielkiej Brytanii Osoba trzecia będzie utrzymywać wykwalifikowany zespół ds. bezpieczeństwa składający się z co najmniej jednego obywatela Wielkiej Brytanii, który będzie dostępny do kontaktów z BT, a zespół ten będzie uczestniczyć w takich spotkaniach, jakich BT będzie od czasu do czasu w uzasadniony sposób wymagać.

16.3 Osoba trzecia dostarczy BT harmonogram (okresowo aktualizowany w razie potrzeby) wszystkich aktywnych komponentów wchodzących w skład Usług i ich odpowiednich źródeł.

16.4 Osoba trzecia zapewni, że instalacja nowych systemów, sprzętu lub oprogramowania we własnej sieci BT wykorzystuje najnowszą wersję oprogramowania i poprawki.

16.5 Osoba trzecia zapewni, że wszystkie istotne dla bezpieczeństwa rejestry są włączone na wszystkich urządzeniach sieciowych zainstalowanych przez Osobę trzecią i wysyłane do sieciowych systemów rejestrowania BT.

16.6 Osoba trzecia dostarczy firmie BT w odpowiednim czasie (tj. tak szybko, jak to możliwe, aby umożliwić usunięcie luk przed ich publicznym opublikowaniem) informacje dotyczące wszelkich luk w zabezpieczeniach Usług oraz spełni (na koszt Osoby trzeciej) takie uzasadnione wymogi dotyczące luk w zabezpieczeniach, jakie mogą zostać zgłoszone przez firmę BT.

16.7 Osoba trzecia zapewni, że wszelkie elementy związane z bezpieczeństwem wchodzące w skład Usług, które są okresowo identyfikowane przez BT lub przekazywane BT, zostaną poddane, na koszt Osoby trzeciej, zewnętrznej ocenie satysfakcjonującej BT.

16.8 Osoba trzecia bezzwłocznie, a w każdym razie w ciągu 7 dni roboczych, przekaże BT szczegółowe informacje na temat wszelkich funkcji i/lub funkcjonalności Usług lub funkcji planowanych w Planie Działania dla Usług, który będzie od czasu do czasu aktualizowany:

- Osoba trzecia o tym wie; lub
- BT ma uzasadnione powody, by sądzić, że są one przeznaczone lub mogą być wykorzystywane do zgodnego z prawem przechwytywania lub innego przechwytywania ruchu telekomunikacyjnego i informuje o tym Osobę trzecią. Takie szczegóły będą obejmować wszelkie Informacje, które są w uzasadniony sposób niezbędne do umożliwienia BT pełnego zrozumienia charakteru, składu i zakresu takich cech i/lub funkcji.

16.9 Osoba trzecia nie może używać żadnych narzędzi do monitorowania sieci, które mogą wyświetlać informacje o aplikacji.

16.10 Personel Osoby trzeciej budujący, rozwijający i/lub obsługujący własną sieć BT musi przejść kontrolę przed zatrudnieniem na poziomie co najmniej L2. Kontrole przed zatrudnieniem na poziomie L3 będą wymagane w przypadku ról określonych przez BT.

16.11 Osoba trzecia zezwoli BT na instalację oprogramowania zabezpieczającego zgodnego ze specyfikacją BT w dowolnej infrastrukturze wirtualnej Osoby trzeciej (w tym m.in. maszynach wirtualnych i kontenerach) lub systemie operacyjnym zainstalowanym przez Osobę trzecią działającym w Sieciach BT.

16.12 Osoba trzecia musi zapewnić, że najnowsze poprawki zabezpieczeń są stosowane do systemów/ zasobów/sieci/aplikacji, zapewniając, że:

- Osoba trzecia wdraża poprawki tak szybko, jak to możliwe, i dokłada wszelkich starań, aby wdrożyć je w następujących ramach czasowych po wydaniu poprawki:

	Aktywnie wykorzystywane na wolności	**Wysoki wskaźnik EPSS** Luki w zabezpieczeniach CVSS: > 8.0 (wysoki + krytyczny) EPSS: >= 70% (Wektor ataku sieciowego – patrz część z definicjami)	**Niższy wskaźnik EPSS** Luki w zabezpieczeniach CVSS: > 8.0 (wysoki + krytyczny) EPSS: < 70% (Wektor ataku sieciowego – patrz część z definicjami)	**Inne** (wektor ataku niesieciowego)
Interfejs wyeksponowany na zewnątrz	7 dni	14 dni	30 dni	90 dni
Interfejs wyeksponowany do wewnątrz	7 dni	14 dni	30 dni	90 dni/BAU

- Osoba trzecia wykorzystuje poprawki uzyskane od: dostawców bezpośrednio dla systemów zastrzeżonych i poprawek, które są (i) podpisane cyfrowo lub (ii) zweryfikowane za pomocą skrótu dostawcy (nie wolno używać skrótów MD5) dla pakietu aktualizacji, tak aby poprawka mogła zostać zidentyfikowana jako pochodząca od renomowanej społeczności wsparcia dla oprogramowania typu open source.
- Osoba trzecia testuje wszystkie poprawki na systemach, które dokładnie reprezentują konfigurację docelowych systemów produkcyjnych przed wdrożeniem poprawki do systemów produkcyjnych, a prawidłowe działanie poprawionej usługi jest weryfikowane po każdej czynności związanej z łataniem.
- Monitorowanie wszystkich odpowiednich dostawców i innych istotnych źródeł informacji pod kątem alertów o lukach w zabezpieczeniach.
- Jeśli system nie może zostać załatany, należy wdrożyć odpowiednie środki zaradcze.
- Osoba trzecia będzie dostarczać krytyczne poprawki zabezpieczeń oddzielnie od wydań funkcji, aby zmaksymalizować szybkość, z jaką można wdrożyć poprawkę, i w miarę możliwości będzie nadawać priorytet krytycznym poprawkom zabezpieczeń nad aktualizacjami funkcji.

Ustawa o bezpieczeństwie telekomunikacyjnym z 2021 r. (TSA)

W przypadku, gdy Osoba trzecia dostarcza lub udostępnia towary, usługi lub urządzenia do użytku w związku z publiczną siecią lub usługą łączności elektronicznej w Wielkiej Brytanii, zastosowanie mają następujące środki kontroli bezpieczeństwa.

16.13 W przypadku, gdy Osoba trzecia obsługuje więcej niż jednego operatora, należy wdrożyć kontrole, aby zapobiec negatywnemu wpływowi jednego operatora lub jego sieci na innego operatora lub jego sieć.

16.14 W przypadku, gdy Osoba trzecia działa jako Administrator zewnętrzny dla więcej niż jednego operatora, zastosowanie mają następujące kontrole:

- Wdrożenie logicznej separacji w sieci Osoby trzeciej w celu oddzielenia danych klientów i sieci.
- Wdrożenie separacji między środowiskami zarządzania innych firm używanymi w sieciach różnych operatorów.
- Wdrażanie i egzekwowanie funkcji wymuszających bezpieczeństwo na granicy między siecią osoby trzeciej a siecią operatora.
- Wdrożenie kontroli technicznych w celu ograniczenia możliwości negatywnego wpływu użytkowników lub systemów na więcej niż jednego operatora.
- Wdrożenie fizycznie i logicznie niezależnych stacji roboczych z dostępem uprzywilejowanym na operatora.
- Wdrożenie niezależnych domen administracyjnych i kont dla każdego operatora.

16.15 Dostarczając sprzęt sieciowy, Osoby trzecie muszą dostarczyć BT „deklarację bezpieczeństwa" dotyczącą sposobu produkcji bezpiecznego sprzętu oraz sposobu zapewnienia bezpieczeństwa sprzętu przez cały okres jego eksploatacji. Deklaracja bezpieczeństwa powinna obejmować wymogi Oceny Bezpieczeństwa Sprzedawcy opublikowanej w Załączniku B do Kodeksu Postępowania w Zakresie Bezpieczeństwa Telekomunikacyjnego i powinna zostać zatwierdzona na odpowiednim szczeblu wyższego szczebla uzgodnionym z BT.

16.16 W przypadku, gdy Osoba trzecia dostarcza sprzęt sieciowy, zastosowanie mają następujące kontrole:

- Osoba trzecia gwarantuje, że będzie przestrzegać standardu nie niższego niż opublikowana przez nią „deklaracja bezpieczeństwa".
- Osoba trzecia dostarczy aktualne wytyczne dotyczące bezpiecznego wdrażania sprzętu.
- Osoba trzecia będzie wspierać cały sprzęt oraz wszystkie podkomponenty oprogramowania i sprzętu przez cały okres obowiązywania umowy.
- Osoby trzecie dostarczą szczegółowych informacji na temat wszystkich głównych komponentów i zależności, w tym między innymi produktu i wersji, komponentów open source oraz poziomu i okresu wsparcia.
- Osoba trzecia usunie wszystkie luki w zabezpieczeniach, które stanowią zagrożenie dla sieci lub usług BT, wykryte w jej produktach, w rozsądnym terminie od otrzymania powiadomienia, zapewniając regularne aktualizacje postępów w międzyczasie – taki czas zostanie uzgodniony między BT i Osobą trzecią, działającymi w sposób rozsądny. Obejmuje to wszystkie produkty, na które podatność ma wpływ, a nie tylko produkt, dla którego podatność została zgłoszona.
- Osoba trzecia usunie lub zmieni domyślne hasła i domyślne lub zakodowane na stałe konta lub zapewni, że sprzęt sieciowy jest skonfigurowany tak, aby umożliwić BT takie działanie.
- Osoba trzecia w miarę możliwości wyłączy niezaszyfrowane protokoły zarządzania, a jeśli nie będzie to możliwe, wskaże BT obecność takich protokołów, aby umożliwić ograniczenie ich użycia.

16.17 Jeśli Osoba trzecia uzyskała uznawane międzynarodowo oceny bezpieczeństwa lub certyfikaty dla sprzętu (np. Common Criteria lub NESAS), udostępni BT pełne ustalenia potwierdzające tę ocenę lub certyfikat.

16.18 W przypadku, gdy własna sieć Osoby trzeciej może mieć wpływ na Sieci BT, Osoba trzecia, zgodnie z zaleceniami BT, zostanie poddana testom na takim samym poziomie, jaki BT stosuje do Sieci BT i usunie zidentyfikowane luki w zabezpieczeniach zgodnie z ustaleniami obu stron.

16.19 Osoba trzecia upoważnia BT do dzielenia się szczegółowymi informacjami na temat kwestii bezpieczeństwa w stosownych przypadkach, gdy jest to konieczne do celów bezpieczeństwa sieci.

16.20 Infrastruktura i systemy wykorzystywane do utrzymania sieci BT muszą być zlokalizowane w Wielkiej Brytanii.

16.21 W przypadku, gdy Osoba trzecia pełni Funkcje Nadzoru Sieci BT, sprzęt wykorzystywany do pełnienia tej funkcji musi być zlokalizowany w Wielkiej Brytanii i obsługiwany przez personel z Wielkiej Brytanii.

16.22 W przypadku, gdy Osoba trzecia jest odpowiedzialna za bezpieczeństwo sieci i dzienniki audytu, będą one przechowywane w Wielkiej Brytanii i chronione zgodnie z prawem brytyjskim.

16.23 W przypadku, gdy Osoba trzecia działa jako Administrator Osoby trzeciej, BT zachowuje prawo do określania uprawnień do kont używanych przez Osobę trzecią w celu uzyskania dostępu do jej sieci oraz do żądania wszystkich dzienników dotyczących bezpieczeństwa sieci Osoby trzeciej w zakresie, w jakim dzienniki te odnoszą się do dostępu do sieci BT. Osoba trzecia będzie monitorować i kontrolować działania swoich pracowników podczas uzyskiwania dostępu do sieci BT.

17. Bezpieczeństwo sieci osób trzecich

17.1 Osoba trzecia musi zapewnić ustanowienie i utrzymanie integralności sieci poprzez zapewnienie odpowiedniej kontroli następujących elementów i powiadomienie BT w każdym przypadku, gdy nie jest to technicznie możliwe:

- Zewnętrzne połączenia z siecią są dokumentowane, przekierowywane przez zaporę sieciową oraz weryfikowane i zatwierdzane przed nawiązaniem połączenia, aby zapobiec naruszeniom bezpieczeństwa danych.
- Sieć jest odpowiednio zaprojektowana przy użyciu zasad „obrony w głąb”, aby zapewnić zminimalizowanie naruszeń cyberbezpieczeństwa poprzez zapewnienie odpowiednich środków kontroli, które zapobiegają wszelkim celowym atakom, takim jak „segmentacja sieci”.
- Projekt i wdrożenie sieci są poddawane przeglądowi co najmniej raz w roku.
- Cały bezprzewodowy dostęp do sieci podlega autoryzacji, uwierzytelnianiu, segmentacji i protokołom szyfrowania, aby zapobiec naruszeniom bezpieczeństwa.
- Korzystanie z bezpiecznej komunikacji między urządzeniami i stacjami zarządzającymi.
- Korzystanie z bezpiecznej komunikacji między urządzeniami, w tym szyfrowanie całego dostępu administratora innego niż konsola.

- Korzystanie z solidnych projektów architektonicznych, które są warstwowe i strefowe z efektywnym zarządzaniem tożsamością i konfiguracją systemu operacyjnego, które muszą być odpowiednio wzmocnione i udokumentowane.
- Poprzez wyłączenie (tam, gdzie to możliwe) usług, aplikacji i portów, które nie będą używane.
- Poprzez wyłączenie lub usunięcie kont gości.
- Poprzez unikanie relacji zaufania między serwerami.
- Wykorzystanie zasady bezpieczeństwa „najmniejszych uprawnień" do wykonywania funkcji.
- Zapewnienie odpowiednich środków wykrywania i/lub ochrony przed włamaniami.
- W stosownych przypadkach monitorowanie integralności plików w celu wykrycia wszelkich dodatków, modyfikacji lub usunięć krytycznych plików systemowych lub danych.
- Zmiana wszystkich domyślnych i dostarczonych przez dostawcę haseł przed uruchomieniem komponentów sieciowych.
- Wyłączenie nieszyfrowanych protokołów zarządzania, jeśli jest to technicznie możliwe.

17.2 Sieć Osoby trzeciej musi spełniać wszystkie wymogi prawne i regulacyjne:

- należy dołożyć wszelkich starań, aby uniemożliwić nieupoważnionym osobom (np. hakerom) uzyskanie dostępu do sieci podmiotów zewnętrznych.
- należy dołożyć wszelkich starań, aby zmniejszyć ryzyko niewłaściwego korzystania z sieci osób trzecich przez osoby upoważnione do dostępu do nich.
- należy dołożyć wszelkich starań w celu wykrycia wszelkich naruszeń bezpieczeństwa i zapewnienia szybkiej naprawy wszelkich naruszeń, wraz z identyfikacją osób, które uzyskały dostęp i ustaleniem, w jaki sposób go uzyskały.

Ustawa o bezpieczeństwie telekomunikacyjnym 2021

17.3 W przypadku, gdy Osoba trzecia dostarcza lub udostępnia towary, usługi lub urządzenia do użytku w związku z publiczną siecią lub usługą łączności elektronicznej w Wielkiej Brytanii, zastosowanie mają następujące dodatkowe środki kontroli bezpieczeństwa:

- Zewnętrzne systemy, z wyłączeniem urządzeń CPE (Customer Premises Equipment), są testowane pod kątem bezpieczeństwa co dwa lata lub w przypadku istotnych zmian.
- Zbiory danych wrażliwych i wrażliwe lub krytyczne funkcje nie są hostowane na urządzeniach na Exposed Edge sieci.
- Jeśli nie są chronione kryptograficznie, należy wdrożyć fizyczną i logiczną separację między odsłoniętą krawędzią a wrażliwymi lub krytycznymi funkcjami.
- Pomiędzy Exposed Edge a funkcjami wrażliwymi lub krytycznymi należy wdrożyć separację zabezpieczeń przy użyciu funkcji wymuszających bezpieczeństwo.

18. Bezpieczeństwo w chmurze

18.1 Podmiot zewnętrzny musi być certyfikowany zgodnie z najnowszą wersją normy ISO27017 lub posiadać ustanowione i spójne ramy zapewniające, że wszelkie wykorzystanie technologii chmury i danych niepublicznych przechowywanych w chmurze jest zatwierdzone i podlega odpowiednim kontrolom równoważnym z najnowszą wersją Cloud Security Alliance, Cloud Controls Matrix (CCM).

18.2 Umowy dotyczące poziomu usług sieciowych i infrastrukturalnych (wewnętrznych lub zewnętrznych) powinny jasno dokumentować wspólne obowiązki, kontrole bezpieczeństwa, przepustowość i poziomy usług oraz wymagania biznesowe lub klienta.

18.3 Osoba trzecia musi wdrożyć środki bezpieczeństwa we wszystkich aspektach świadczonej usługi, tak aby zapewnić poufność, dostępność, jakość i integralność poprzez zminimalizowanie możliwości uzyskania dostępu do Informacji BT i usług wykorzystywanych przez BT przez osoby nieupoważnione (np. innych klientów usług w chmurze).

18.4 W zakresie, w jakim Osoba trzecia udostępnia firmie BT hostowane aplikacje lub usługi, zarówno jedno-, jak i wielodzierżawne, w tym oprogramowanie jako usługę, platformę jako usługę, infrastrukturę jako usługę i podobne oferty, w celu gromadzenia, przesyłania, przechowywania lub przetwarzania w inny sposób Danych poufnych, Osoba trzecia zapewni firmie BT możliwość:

- logicznego odizolowania takich Danych poufnych od danych innych klientów Osoby trzeciej.
- ograniczania, rejestrowania i monitorowania dostępu do takich Danych poufnych w dowolnym momencie, w tym dostępu przez Personel Osoby trzeciej.
- tworzenia, włączania, wyłączania i usuwania najwyższego klucza szyfrowania (znanego jako klucz zarządzany przez klienta) używanego do szyfrowania i odszyfrowywania kolejnych kluczy, w tym najniższego klucza szyfrowania danych.
- ograniczania, rejestrowania i monitorowania dostępu do klucza zarządzanego przez klienta w dowolnym momencie; i w żadnym momencie żaden kolejny klucz szyfrujący, klucz szyfrujący w hierarchii kluczy niższej niż klucz zarządzany przez klienta, nie będzie przechowywany w tym samym systemie co Dane poufne, chyba że zostanie zaszyfrowany przez klucz zarządzany przez klienta, zwany również kluczem opakowanym przez klucz zarządzany przez klienta.

19. Karty SIM

19.1 W przypadku, gdy Osoba trzecia dostarcza karty SIM, zastosowanie mają następujące kontrole:

- w przypadku kart SIM o stałym profilu, Osoba trzecia zapewni, że poufne dane karty SIM są odpowiednio chronione przez producenta karty SIM.
- w przypadku kart SIM o stałym profilu Osoba trzecia zapewni ochronę poufności, integralności i dostępności wrażliwych danych karty SIM udostępnianych producentowi karty SIM na każdym etapie ich cyklu życia.

20. Informacje sklasyfikowane jako URZĘDOWE lub o wyższym stopniu poufności przez HMG

20.1 Dodatkowe wymogi bezpieczeństwa określone w Załączniku 1 do niniejszych Wymogów bezpieczeństwa będą miały zastosowanie do każdej Osoby trzeciej, która będzie przechowywać, przetwarzać lub przekazywać informacje zaklasyfikowane jako URZĘDOWE zgodnie z Systemem Klasyfikacji Bezpieczeństwa Rządu Jego Królewskiej Mości (His Majesty's Government Security Classifications Scheme), aktualizowanym od czasu do czasu.

21. Zdefiniowane terminy i interpretacja

21.1 O ile poniżej nie określono inaczej, słowa i wyrażenia użyte w niniejszych Wymogach bezpieczeństwa będą miały takie samo znaczenie jak w Umowie:

„**Dostęp**" i „**Uzyskanie dostępu**" oznaczają Przetwarzanie, obsługę lub przechowywanie Informacji BT za pomocą jednej lub kilku z poniższych metod:

a. poprzez połączenie z Systemami BT;

b. w formie papierowej lub nieelektronicznej;

c. Informacje BT o systemach dostawców; lub

d. przez media mobilne

i/lub Dostęp do pomieszczeń BT w celu zapewnienia Dostaw, z wyłączeniem dostawy sprzętu i uczestnictwa w spotkaniach.

„**Informacje BT**" oznaczają wszelkie Informacje dotyczące BT lub Klienta BT przekazane Dostawcy oraz wszelkie Informacje przetwarzane lub obsługiwane przez Dostawcę w imieniu BT lub Klienta BT na podstawie Umowy.

„Interesariusz BT" oznacza przedstawiciela BT, który jest właścicielem zakresu prac wykonywanych przez Osobę trzecią.

„**Systemy BT**" oznaczają Usługi i komponenty Usług, produkty, sieci, serwery, procesy, systemy papierowe lub systemy IT (w całości lub w części) będące własnością i/lub obsługiwane przez BT lub takie inne systemy, które mogą być hostowane w obiektach BT.

„Sieci BT" " oznaczają każdą Publiczną Sieć Łączności Elektronicznej obsługiwaną przez BT, zgodnie z definicją zawartą w sekcji 32 Ustawy o łączności z 2003 r. (Communications Act 2003).

„BYOD" oznacza „przynieś własne urządzenie".

„**Umowa**" oznacza Umowę zawartą przez Osoby na dostawę towarów, oprogramowania lub Usług, która odwołuje się do niniejszych Wymagań bezpieczeństwa.

„Sprzęt w lokalu klienta" oznacza sprzęt dostarczany klientom przez dostawcę i zarządzany przez dostawcę, który jest używany lub ma być używany jako część sieci lub usługi. Nie obejmuje to konsumenckich urządzeń elektronicznych, takich jak telefony komórkowe i tablety, ale obejmuje urządzenia takie jak zapory brzegowe, sprzęt SD-WAN i stacjonarny zestaw dostępu bezprzewodowego. ""

„**Cyber Essentials Plus**" oznacza program wspierany przez rząd Wielkiej Brytanii, który pomaga organizacjom chronić się przed powszechnymi cyberatakami.

„Cyberbezpieczeństwo” oznacza sposób, w jaki osoby fizyczne i organizacje zmniejszają ryzyko cyberataku. Podstawową funkcją cyberbezpieczeństwa jest ochrona urządzeń, z których wszyscy korzystamy (smartfonów, laptopów, tabletów i komputerów) oraz usług, do których mamy dostęp – zarówno online, jak i w pracy – przed kradzieżą lub uszkodzeniem.

„EPSS” oznacza System punktacji przewidywania ataków (Exploit Prediction Scoring System).

„**Umowa powiernicza**” oznacza umowę depozytu kodu źródłowego zawartą zgodnie z Umową w celu używania, kopiowania, utrzymywania i modyfikowania takiego kodu źródłowego do celów biznesowych BT (w tym prawo do kompilacji takiego kodu źródłowego).

„**Odsłonięty brzeg**” oznacza sprzęt, który znajduje się w lokalu klienta, jest bezpośrednio adresowalny z poziomu sprzętu klienta/użytkownika lub jest fizycznie podatny na uszkodzenia. Fizycznie wrażliwy sprzęt obejmuje sprzęt w szafkach przydrożnych lub przymocowany do mebli ulicznych. Odsłonięte urządzenie brzegowe obejmuje CPE, sprzęt stacji bazowej, sprzęt OLT i sprzęt MSAN/DSLAM.

„**Dobra praktyka bezpieczeństwa branżowego**” oznacza, w odniesieniu do dowolnego przedsiębiorstwa i dowolnych okoliczności, wdrożenie praktyk bezpieczeństwa, polityk, standardów i narzędzi, których można by racjonalnie i zwyczajowo oczekiwać od wykwalifikowanej i doświadczonej osoby zaangażowanej w ten sam rodzaj działalności w tych samych lub podobnych okolicznościach.

„NDA” oznacza umowę o zachowaniu poufności, która jest wiążącą umową między dwiema lub więcej stronami, a która zapobiega udostępnianiu poufnych informacji innym osobom.

„NESAS” oznacza program zapewnienia bezpieczeństwa sprzętu sieciowego GSM Association.

„Zasób sieciowy” oznacza element, który jest częścią zbioru połączonych ze sobą komponentów, takich jak komputery, routery, koncentratory, okablowanie i kontrolery telekomunikacyjne, które tworzą sieć.

„Wektor ataku sieciowego” oznacza, że podatny komponent jest powiązany ze stosem sieciowym, a zestaw możliwych napastników wykracza poza inne opcje wymienione poniżej, aż do całego Internetu włącznie. Takie luki w zabezpieczeniach są często określane jako „możliwe do zdalnego wykorzystania” i mogą być traktowane jako atak możliwy do wykorzystania na poziomie protokołu w odległości jednego lub więcej przeskoków sieciowych (np. przez jeden lub więcej routerów). Przykładem ataku sieciowego jest atakujący powodujący odmowę usługi (DoS) poprzez wysłanie specjalnie spreparowanego pakietu TCP przez sieć rozległą (np. CVE 2004 0230).

„Funkcja nadzoru sieci” oznacza elementy Sieci BT, które nadzorują i kontrolują funkcje krytyczne dla bezpieczeństwa, co czyni je niezwykle ważnymi dla ogólnego bezpieczeństwa sieci. Są one niezbędne, aby firma BT mogła zrozumieć sieć, zabezpieczyć sieć lub odzyskać sieć.

„**Bezpieczeństwo sieci**” oznacza bezpieczeństwo wzajemnie połączonych ścieżek komunikacyjnych i węzłów, które logicznie łączą ze sobą technologie użytkownika końcowego i powiązane systemy zarządzania.

„NIST” oznacza Narodowy Instytut Standardów i Technologii – jednostkę Departamentu Handlu Stanów Zjednoczonych. Wcześniej znany jako National Bureau of Standards,

NIST promuje i utrzymuje standardy pomiarowe. Prowadzi również aktywne programy zachęcające i pomagające przemysłowi i nauce w opracowywaniu i stosowaniu tych standardów.

„**Oficjalna Deklaracja Wrażliwości**" oznacza pisemną deklarację Dostawcy dotyczącą ról zidentyfikowanych przez Dostawcę jako posiadające dostęp do informacji sklasyfikowanych jako „Oficjalne wrażliwe" lub posiadające podwyższone uprawnienia do infrastruktury, która przechowuje, przetwarza lub przesyła informacje sklasyfikowane jako „Oficjalne wrażliwe", której wzór znajduje się w Załączniku 1.

„Stacja robocza z dostępem uprzywilejowanym (PAW)" oznacza stacje robocze, za pośrednictwem których możliwy jest dostęp uprzywilejowany.

„Funkcja krytyczna dla bezpieczeństwa" oznacza dowolną funkcję Sieci lub Usługi BT, której działanie może mieć istotny wpływ na prawidłowe działanie całej sieci lub usługi lub ich istotnej części.

„**Wymogi bezpieczeństwa**" oznaczają niniejszy dokument aktualizowany od czasu do czasu.

„SIM" oznacza unikalny komponent sprzętowy lub token oraz związane z nim oprogramowanie, używane do uwierzytelniania dostępu abonenta do sieci. W rozumieniu niniejszego dokumentu karta SIM obejmuje sprzętową kartę UICC/eUICC, aplikacje SIM/USIM/ISIM, funkcje eSIM i RSP oraz wszelkie aplety SIM.

„**Podwykonawca**" oznacza Podwykonawcę Dostawcy, który wykonuje lub jest zaangażowany w dostarczanie Dostaw lub który zatrudnia lub angażuje osoby zaangażowane w dostarczanie Dostaw.

„**Usługa**" oznacza wszelkie „**Towary**", "**Oprogramowanie**" lub „**Usługi**" zgodnie z definicją w Umowie.

„Transakcja" oznacza dane transakcyjne / informacje, które są przechwytywane z transakcji, tj. dane generowane przez różne aplikacje podczas uruchamiania lub wspierania codziennych procesów biznesowych.

„Moduł zaufanej platformy" oznacza technologię zaprojektowaną w celu zapewnienia sprzętowych funkcji związanych z bezpieczeństwem. Moduł TPM to bezpieczny procesor kryptograficzny przeznaczony do wykonywania operacji kryptograficznych. Chip zawiera wiele fizycznych mechanizmów bezpieczeństwa, dzięki czemu jest odporny na manipulacje, a złośliwe oprogramowanie nie jest w stanie manipulować funkcjami bezpieczeństwa modułu TPM. Najpopularniejsze funkcje TPM są wykorzystywane do pomiarów integralności systemu oraz do tworzenia i używania kluczy. Podczas procesu uruchamiania systemu ładowany kod rozruchowy (w tym oprogramowanie układowe i składniki systemu operacyjnego) może być mierzony i rejestrowany w module TPM. Pomiary integralności mogą być wykorzystane jako dowód na to, w jaki sposób system został uruchomiony i aby upewnić się, że klucz oparty na module TPM został użyty tylko wtedy, gdy do uruchomienia systemu użyto właściwego oprogramowania.

„Osoba trzecia" oznacza Dostawcę BT.

„Administrator zewnętrzny" oznacza dostawcę usług zarządzanych, dostawcę funkcji grupowych lub zewnętrznego wsparcia dla sprzętu dostawcy zewnętrznego (np. funkcja wsparcia trzeciej linii).

„**Personel Osoby trzeciej**" oznacza wszelkie osoby zaangażowane przez Dostawcę lub jego Podwykonawców w wykonywanie zobowiązań Dostawcy wynikających z Umowy.

„Sieć Osoby trzeciej” oznacza dowolną sieć Dostawcy.

"**System Osoby trzeciej**” oznacza każdy należący do Dostawcy komputer, aplikację lub system sieciowy wykorzystywany do uzyskiwania dostępu, przechowywania lub przetwarzania Informacji BT lub zaangażowany w świadczenie Dostaw.

Interpretacja

21.2 Wszelkie słowa następujące po terminach „w tym”, „w tym”, „w szczególności”, „na przykład” lub podobnych wyrażeniach będą interpretowane jako ilustracyjne i nie będą ograniczać sensu słów, opisu, definicji, frazy lub terminu poprzedzającego te terminy.

21.3 Za każdym razem, gdy prawo lub zobowiązanie Osoby jest wyrażone jako takie, które „**może**” ona wykonać, opcja zrealizowania lub wykonania tego prawa lub zobowiązania będzie leżeć w wyłącznej gestii tej Osoby.

21.4 W przypadku odniesienia do jakiegokolwiek hiperłącza („**URL**”), takie odniesienie będzie dotyczyło takiego zasobu internetowego dostępnego za pośrednictwem tego adresu URL lub innego zastępczego adresu URL, o którym dana Osoba jest okresowo powiadamiana.

Wersja	Opis	Autor	Data
5.0	Ustawa o bezpieczeństwie telekomunikacji z 2021 r. (TSA) i przyjęcie CIS przez BT	Jemma Turner	25/10/22
5.1	Poprawka do 14.9 TLS	Jemma Turner	17/04/23
5.2	Zmiany w różnych klauzulach w celu uwzględnienia TSA i luk w zabezpieczeniach	Jemma Turner	30/11/23

ZAŁĄCZNIK 1 - Dodatkowe wymogi bezpieczeństwa

W przypadku, gdy Osoba trzecia jest zobowiązana do uzyskiwania dostępu, przechowywania, przetwarzania lub przekazywania informacji niejawnych o klauzuli URZĘDOWE lub wyższej, Osoba trzecia będzie przestrzegać Wymogów bezpieczeństwa BT oraz dodatkowo wymogów określonych w niniejszym Załączniku 1. We wszystkich przypadkach kontrola najwyższego poziomu będzie nadrzędna w stosunku do wymogów udokumentowanych w innych częściach niniejszych Wymogów bezpieczeństwa.

1. PRACOWNICY

1.1 Wszyscy zatrudnieni pracownicy Osoby trzeciej mający dostęp do informacji niejawnych o klauzuli tajności URZĘDOWE lub wyższej lub posiadający podwyższone uprawnienia do infrastruktury, która przechowuje, przetwarza lub przesyła informacje niejawne o klauzuli tajności URZĘDOWE lub wyższej:

1.1.1 muszą zostać poddani kontroli przed zatrudnieniem zgodnie z normą Baseline Personnel Security Standard (BPSS) jako minimum;

1.1.2 muszą podpisać oświadczenie zgodnie z ustawą o tajemnicy służbowej; oraz

1.1.3. muszą mieć uniemożliwiony dostęp do informacji lub systemów, chyba że posiadają wymagane poświadczenia bezpieczeństwa określone w odpowiedniej umowie.

2. SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA

2.1. Osoba trzecia zleci przeprowadzenie szkolenia w zakresie bezpieczeństwa po zatrudnieniu i co najmniej raz w roku dla wszystkich pracowników mających dostęp do informacji niejawnych o klauzuli URZĘDOWE lub wyższej lub posiadających podwyższone uprawnienia do infrastruktury, która przechowuje, przetwarza lub przesyła informacje niejawne o klauzuli URZĘDOWE lub wyższej. Szkolenie to obejmie wymogi dotyczące przetwarzania informacji zgodnie z wymogami Systemu Klasyfikacji Bezpieczeństwa Rządu Jego Królewskiej Mości, wyszczególnionymi w dokumencie BT Protecting HMG Information Guidance for 3rd Parties, który zostanie dostarczony Osobie trzeciej przez BT.

2.2. Osoba trzecia zaktualizuje opisy stanowisk dla wszystkich pracowników mających dostęp do informacji niejawnych o klauzuli URZĘDOWE lub wyższej lub posiadających podwyższone uprawnienia do infrastruktury, która przechowuje, przetwarza lub przesyła informacje niejawne o klauzuli URZĘDOWE lub wyższej, w celu upoważnienia do udziału w szkoleniu opisanym w punkcie 2.1 powyżej. Osoba trzecia będzie prowadzić rejestr szkoleń, który musi zostać udostępniony BT na żądanie.

3. KONTROLA DOSTĘPU

3.1. Gdy pracownicy odchodzą lub zmieniają role, ich prawa dostępu muszą zostać cofnięte z odpowiednich systemów osób trzecich w ciągu 1 dnia roboczego.

3.2. W przypadku, gdy pracownicy Osoby trzeciej, w tym wykonawcy, pracownicy tymczasowi i pracownicy agencyjni, mają podwyższone uprawnienia do infrastruktury BT, Osoba trzecia musi powiadomić BT na piśmie w ciągu 1 dnia roboczego od momentu, gdy pracownik nie wymaga już dostępu do Systemów BT (np. odejście pracownika lub zmiana stanowiska).

3.3. W przypadku, gdy pracownikom Osoby trzeciej, w tym wykonawcom, pracownikom tymczasowym i pracownikom agencyjnym, wydawane są stałe karty dostępu do obiektów BT, Osoba trzecia musi powiadomić BT na piśmie w ciągu 1 dnia roboczego, gdy pracownik nie wymaga już dostępu do obiektów BT (np. pracownicy odchodzą lub zmieniają stanowisko).

4. WYCENA I KLASYFIKACJA AKTYWÓW

4.1. Osoba trzecia wdroży dodatkowe procedury postępowania z informacjami w celu spełnienia wymogów postępowania zgodnie z wymogami rządowego programu nadawania klauzul tajności Jego Królewskiej Mości, aktualizowanego co pewien czas.

5. REAGOWANIE NA INCYDENTY I RAPORTOWANIE - UMOWY O GWARANTOWANYM POZIOMIE USŁUG

5,1. Osoba trzecia zostanie poinformowana o konkretnych umowach dotyczących poziomu usług w celu wsparcia procesu reagowania na incydenty. Mogą one zastąpić wszelkie wcześniejsze umowy określone w niniejszych Wymogach bezpieczeństwa.

6. AUDYT, TESTOWANIE I MONITOROWANIE

6.1. Osoba trzecia wdroży całodobowy monitoring bezpieczeństwa infrastruktury Osoby trzeciej, która obsługuje przetwarzanie, przechowywanie lub przesyłanie informacji niejawnych o klauzuli URZĘDOWEJ lub wyższej, w przypadkach określonych przez BT.

7. CIĄGŁOŚĆ DZIAŁANIA I ODZYSKIWANIE DANYCH PO AWARII

7.1. Osoba trzecia opracuje plan ciągłości działania i odtwarzania po awarii zgodnie z normą BS ISO 22301 w ciągu 30 dni od podpisania umowy.

8. LOKALIZACJA

8.1. O ile BT nie postanowi inaczej, Usługa musi być fizycznie zlokalizowana w granicach Wielkiej Brytanii lub, w stosownych przypadkach, EOG. Jakiekolwiek zdalne wsparcie i/lub zarządzanie Usługą przez Dostawcę z lokalizacji zagranicznej będzie realizowane wyłącznie zgodnie z procesem zatwierdzania określonym w obowiązującej umowie pomiędzy BT a danym departamentem rządowym.

9. DODATKOWE WYMOGI DLA DANYCH O STATUSIE URZĘDOWE-WRAŻLIWE LUB WYŻSZYM

Wszystkie role zidentyfikowane przez Osobę trzecią jako posiadające dostęp do informacji o klauzuli tajności URZĘDOWE-WRAŻLIWE lub wyższej lub posiadające podwyższone uprawnienia do infrastruktury, która przechowuje, przetwarza lub przesyła informacje o klauzuli tajności URZĘDOWE-WRAŻLIWE lub wyższej, zostaną udokumentowane w Oświadczeniu URZĘDOWE-WRAŻLIWE i dostarczą BT wypełnione Oświadczenie URZĘDOWE-WRAŻLIWE przed podpisaniem Umowy.

9.2 W przypadku, gdy od Dostawcy wymaga się dostępu, przechowywania, przetwarzania lub przekazywania informacji o klauzuli tajności HMG URZĘDOWE-WRAŻLIWE lub wyższej, Dostawca przeprowadzi Ocenę ryzyka bezpieczeństwa personelu dla wszystkich ról określonych w Deklaracji statusu danych „URZĘDOWE-WRAŻLIWE" ust. 2 zgodnie z wymogami określonymi w dokumencie National Protective Security Authority (NPSA) Personnel Security Risk assessment - A guide (wydanie 4 – czerwiec 2013 r. lub późniejsze).

ANEKS 1, ZAŁĄCZNIK 1 - WZÓR DEKLARACJI statusu danych „URZĘDOWE-WRAŻLIWE”

1. Systemy/usługi objęte deklaracją

Należy wymienić systemy i usługi świadczone na rzecz klienta HMG.

System	Usługa

2. Stanowiska osób trzecich wymagające poświadczenia bezpieczeństwa.

Stanowisko	Wymagany poziom poświadczenia bezpieczeństwa
* np. DBA	SC

3. Zarządzanie lukami w zabezpieczeniach

System	Rodzaj oceny luk w zabezpieczeniach	Częstotliwość

4. Audyt, testowanie i monitorowanie

Systemy podlegające monitorowaniu całodobowemu (24/7) zgodnie z zaleceniami BT.

ANEKS 2, Ustawa o telekomunikacji (bezpieczeństwo) z 2021 r. - Kodeks postępowania w zakresie konwersji wymogów bezpieczeństwa

Numeracja kodów	Wymóg	Klauzula wymogów bezpieczeństwa BT
M1.02	Testy bezpieczeństwa systemów zewnętrznych, z wyłączeniem CPE, powinny być zwykle przeprowadzane co najmniej raz na dwa lata, a w każdym razie wkrótce po wystąpieniu znaczącej zmiany.	17.3
M1.03	Urządzenia na odsłoniętym brzegu nie mogą zawierać wrażliwych danych ani funkcji krytycznych dla bezpieczeństwa.	17.3
M1.04	Należy wdrożyć fizyczną i logiczną separację między narażoną krawędzią a funkcjami krytycznymi dla bezpieczeństwa. Należy zauważyć, że środek ten może nie być konieczny, gdy zbiory danych i funkcje mogą być chronione kryptograficznie przed naruszeniem bezpieczeństwa.	17.3
M1.05	Pomiędzy odsłoniętym brzegiem a krytycznymi lub wrażliwymi funkcjami, które wdrażają środki ochronne, muszą istnieć granice bezpieczeństwa.	17.3
M2.02	Cały uprzywilejowany dostęp powinien być rejestrowany.	3.56, 3.57
M2.06	Za infrastrukturę wykorzystywaną do obsługi sieci dostawcy odpowiada dostawca lub inny podmiot, który przestrzega przepisów, środków i nadzoru w zakresie, w jakim mają one zastosowanie do dostawcy (np. dostawca zewnętrzny, z którym dostawca ma stosunek umowny). W przypadku gdy odpowiedzialność ponosi dostawca lub inny podmiot przestrzegający przepisów, odpowiedzialność ta obejmuje zachowanie nadzoru nad zarządzaniem tą infrastrukturą (w tym wgląd w działania zarządcze, personel, któremu przyznano dostęp do zarządzania, oraz procesy zarządzania).	3.56, 3.57 i 4, 14
M5.05	Dostawcy przeprowadzają analizę przyczyn źródłowych wszystkich incydentów związanych z bezpieczeństwem. Wyniki tej analizy będą eskalowane na odpowiedni poziom, który może obejmować zarząd dostawcy.	3.36
M6.01	Nietrwałe dane uwierzytelniające (np. nazwa użytkownika i hasło) powinny być przechowywane w scentralizowanej usłudze z odpowiednią kontrolą dostępu opartą na rolach, która powinna być aktualizowana zgodnie z wszelkimi odpowiednimi zmianami ról i obowiązków w organizacji.	3.44
M6.02	Uprzywilejowany dostęp odbywa się za pośrednictwem kont z unikalnym identyfikatorem użytkownika i danymi uwierzytelniającymi dla każdego użytkownika, które nie mogą być udostępniane.	3.47

M6.04	Wszystkie uprzywilejowane konta użytkowników (typu „break-glass”) muszą mieć unikalne, silne poświadczenia dla każdego urządzenia sieciowego.	3.48
M6.05	Domyślne i zakodowane konta powinny być wyłączone.	16.16
M8.05	Dostawcy powinni rejestrować wszystkie urządzenia wdrożone w ich sieciach i proaktywnie oceniać, co najmniej raz w roku, swoją ekspozycję na wypadek, gdyby dostawca zewnętrzny nie był w stanie nadal obsługiwać tego sprzętu.	16.16, 16.5
M8.06	Dostawcy usuwają lub zmieniają domyślne hasła i konta dla wszystkich urządzeń w sieci i powinni wyłączyć nieszyfrowane protokoły zarządzania. Jeśli nie można wyłączyć nieszyfrowanych protokołów zarządzania, dostawcy powinni ograniczyć i złagodzić korzystanie z tych protokołów tak dalece, jak to możliwe.	16.16 i 17.1
M8.07	Dostawcy zapewniają, że wszystkie istotne dla bezpieczeństwa rejestry są włączone na wszystkich urządzeniach sieciowych i wysyłane do sieciowych systemów rejestrowania.	16.5
M8.08	W miarę możliwości dostawcy powinni traktować priorytetowo krytyczne poprawki zabezpieczeń w stosunku do aktualizacji funkcjonalności.	14.1 i 16.12
M8.12	W przypadku kart SIM o stałym profilu dostawca zapewnia, że wrażliwe dane SIM są odpowiednio chronione przez cały cykl ich życia, zarówno przez dostawcę karty SIM, jak i w sieci operatora, biorąc pod uwagę ryzyko dla odporności sieci i poufności w przypadku utraty tych informacji.	19.1
M8.13	W przypadku kart SIM o stałym profilu poufność, integralność i dostępność wrażliwych danych karty SIM udostępnianych dostawcy karty SIM muszą być chronione na każdym etapie ich cyklu życia.	19.1
M10.04	Proces zarządzania incydentami dostawcy i jego dostawców zewnętrznych powinien zapewniać wzajemne wsparcie w rozwiązywaniu incydentów.	3.31-3.36
M10.06	Dostawca określa, jakie informacje są udostępniane każdemu dostawcy zewnętrznemu, zapewniając, że jest to minimum niezbędne do wypełnienia ich funkcji. Dostawcy umieszczają zabezpieczenia na tych informacjach i ograniczają dostęp osób trzecich do minimum wymaganego do wypełnienia funkcji biznesowej.	3.44
M10.09	W przypadku, gdy dane sieciowe lub dane użytkownika opuszczają kontrolę dostawcy, dostawca powinien umownie wymagać i weryfikować, czy dane są w konsekwencji odpowiednio chronione. Obejmuje to ocenę kontroli dostawcy zewnętrznego w celu zapewnienia, że dane dostawcy są widoczne lub dostępne tylko dla odpowiednich pracowników i z odpowiednich lokalizacji.	3.44-3.50 i 14, 15, 17 oraz 18

M10.11	Dostawcy zobowiązują umownie dostawców zewnętrznych do powiadamiania dostawcy w ciągu 48 godzin od uzyskania informacji o wszelkich incydentach związanych z bezpieczeństwem, które mogły spowodować lub przyczynić się do naruszenia bezpieczeństwa, lub w przypadku gdy zidentyfikują zwiększone ryzyko wystąpienia takiego naruszenia. Obejmuje to między innymi incydenty w sieci deweloperskiej dostawcy lub jego sieci korporacyjnej.	3.33
M10.12	Dostawcy powinni wymagać na mocy umowy, aby dostawcy zewnętrzni wspierali dostawcę w dochodzeniach dotyczących incydentów, które powodują lub przyczyniają się do wystąpienia naruszenia bezpieczeństwa w odniesieniu do głównego dostawcy lub zwiększonego ryzyka wystąpienia takiego naruszenia.	3.31-3.36
M10.13	Dostawcy będą umownie wymagać od dostawców zewnętrznych znalezienia i zgłoszenia pierwotnej przyczyny każdego incydentu bezpieczeństwa, który może skutkować naruszeniem bezpieczeństwa w Wielkiej Brytanii w ciągu 30 dni i naprawienia wszelkich wykrytych błędów w zabezpieczeniach.	3.35
M10.16	Dostawcy zobowiązani są na mocy umowy wymagać od dostawców zewnętrznych wspierania, w odpowiednim zakresie, wszelkich audytów bezpieczeństwa, ocen lub testów wymaganych przez dostawcę w odniesieniu do bezpieczeństwa własnej sieci dostawcy, w tym tych niezbędnych do oceny wymogów bezpieczeństwa w niniejszym dokumencie.	5.1-5.2, 6.1-6.3
M10.18	Dostawca zachowuje prawo do określania uprawnień kont używanych do uzyskiwania dostępu do jego sieci przez administratorów będących osobami trzecimi.	16.23
M10.21	Dostawcy mają umowne prawo do kontrolowania członków personelu zewnętrznego administratora, którzy są zaangażowani w świadczenie usług zewnętrznego administratora, w tym do żądania od zewnętrznego administratora zapewnienia, aby żaden członek personelu nie miał już dostępu do sieci.	13.1
M10.24	Dostawcy będą umownie wymagać, aby administratorzy zewnętrzni wdrożyli kontrole techniczne, aby zapobiec negatywnemu wpływowi jednego dostawcy lub jego sieci na innego dostawcę lub jego sieć.	16.13
M10.25	Dostawcy będą umownie wymagać, aby administratorzy zewnętrzni wdrożyli logiczną separację w sieci administratora zewnętrznego w celu oddzielenia danych i sieci klientów.	16.14
M10.26	Dostawcy będą umownie wymagać, aby administratorzy zewnętrzni wdrożyli separację między środowiskami zarządzania administratorów zewnętrznych używanymi dla różnych sieci dostawców.	16.14
M10.27	Dostawcy będą umownie wymagać, aby administratorzy zewnętrzni wdrażali i egzekwowali funkcje egzekwowania	16.14

	bezpieczeństwa na granicy między siecią administratora zewnętrznego a siecią dostawcy.	
M10.28	Dostawcy powinni umownie wymagać od zewnętrznych administratorów wdrożenia technicznych środków kontroli w celu ograniczenia możliwości negatywnego wpływu użytkowników lub systemów na więcej niż jednego dostawcę.	16.14
M10.29	Dostawcy będą umownie wymagać, aby administratorzy zewnętrzni wdrożyli logicznie niezależne stacje robocze z uprzywilejowanym dostępem dla każdego dostawcy.	16.14
M10.30	Dostawcy będą umownie wymagać od zewnętrznych administratorów wdrożenia niezależnych domen administracyjnych i kont dla każdego dostawcy.	16.14
M10.33	Dostawca wymaga na mocy umowy, aby administrator zewnętrzny monitorował i audytował działania personelu administratora zewnętrznego podczas uzyskiwania dostępu do sieci dostawcy	3.56, 3.57
M10.34	Dostawca wymaga na mocy umowy od zewnętrznego administratora wszystkich dzienników dotyczących bezpieczeństwa sieci zewnętrznego administratora w zakresie, w jakim takie dzienniki odnoszą się do dostępu do sieci dostawcy.	3.56, 3.57 i 16.23
M10.35	Dostawcy będą wymagać, aby sieci zewnętrznego administratora, które mogą mieć wpływ na dostawcę, przechodziły taki sam poziom testów, jaki dostawca stosuje do siebie (np. testy TBEST ustalane dla dostawcy przez Ofcom od czasu do czasu).	16.18
M10.36	Dostawcy powinni na mocy umowy wymagać od dostawców sprzętu sieciowego udostępnienia im „deklaracji bezpieczeństwa” dotyczącej sposobu, w jaki produkują bezpieczny sprzęt i zapewniają utrzymanie bezpieczeństwa sprzętu przez cały okres jego eksploatacji. Zaleca się, aby każda taka deklaracja obejmowała wszystkie aspekty opisane w Vendor Security Assessment (VSA) (patrz Aneks B), a dostawcy powinni zachęcać swoich dostawców do publikowania odpowiedzi na VSA.	16.15
M10.38	Dostawcy zapewniają, w drodze ustaleń umownych, że deklaracja bezpieczeństwa dostawcy sprzętu sieciowego jest podpisywana na odpowiednim poziomie zarządzania.	16.15
M10.39	W przypadku, gdy dostawca sprzętu sieciowego twierdzi, że uzyskał jakiekolwiek uznane międzynarodowo oceny lub certyfikaty bezpieczeństwa swojego sprzętu (takie jak Common Criteria lub NESAS), dostawcy powinni na mocy umowy wymagać od dostawców sprzętu udostępnienia im pełnych ustaleń potwierdzających tę ocenę lub certyfikat.	16.17
M10.40	Dostawcy powinni na mocy umowy wymagać od dostawców sprzętu sieciowego przestrzegania standardu nie niższego niż deklaracja bezpieczeństwa dostawcy sprzętu sieciowego.	16.16

M10.41	Dostawcy powinni wymagać od dostawców sprzętu sieciowego dostarczania aktualnych wytycznych dotyczących sposobu bezpiecznego wdrażania sprzętu.	16.16
M10.42	Dostawcy powinni wymagać od dostawców sprzętu sieciowego wsparcia dla całego sprzętu oraz wszystkich komponentów oprogramowania i sprzętu przez cały okres obowiązywania umowy. Okres wsparcia zarówno dla sprzętu, jak i oprogramowania powinien być zapisany w umowie.	16.16
M10.43	Dostawcy powinni wymagać od dostawców sprzętu sieciowego dostarczenia szczegółowych informacji (produkt i wersja) na temat głównych komponentów i zależności osób trzecich, w tym komponentów open-source oraz okresu i poziomu wsparcia.	16.16
M10.44	Tam, gdzie ma to znaczenie dla konkretnego wykorzystania sprzętu przez dostawcę, dostawcy będą umownie wymagać od dostawców zewnętrznych naprawienia wszystkich kwestii bezpieczeństwa, które stanowią zagrożenie dla bezpieczeństwa sieci lub usługi dostawcy, wykrytych w ich produktach w rozsądnym czasie od powiadomienia, zapewniając regularne aktualizacje postępów w międzyczasie. Obejmuje to wszystkie produkty, na które podatność ma wpływ, a nie tylko produkt, dla którego podatność została zgłoszona.	16.16
M10.46	Dostawcy dopilnowują, aby ich umowy umożliwiały udostępnianie szczegółowych informacji na temat kwestii bezpieczeństwa w celu wspierania identyfikacji i ograniczania ryzyka naruszenia bezpieczeństwa publicznej sieci łączności elektronicznej lub publicznych usług łączności elektronicznej w wyniku działań podjętych lub zaniechanych przez dostawców będących osobami trzecimi.	3.33 i 16.19
M10.47	Dostawcy powinni wymagać od dostawców sprzętu sieciowego dostarczania krytycznych poprawek bezpieczeństwa oddzielnie od wersji funkcji, aby zmaksymalizować szybkość, z jaką można wdrożyć poprawkę.	14.1 i 16.12
M11.02	Wszelkie trwałe dane uwierzytelniające i tajemnice (np. dotyczące dostępu przez szybę) powinny być chronione i niedostępne dla nikogo z wyjątkiem osób odpowiedzialnych w sytuacjach awaryjnych.	3.44
M11.03	Centralne przechowywanie trwałych danych uwierzytelniających powinno być chronione sprzętowo. Na przykład na fizycznym hoście dysk może być zaszyfrowany przy użyciu modułu TPM. W przypadku, gdy maszyna wirtualna (VM) jest używana do świadczenia usługi centralnej pamięci masowej, ta maszyna wirtualna i zawarte w niej dane muszą być również zaszyfrowane; VM musi używać bezpiecznego rozruchu i być skonfigurowana tak, aby zapewnić możliwość uruchomienia tylko w odpowiednim środowisku. Ma to na celu zapewnienie, że dane nie mogą zostać usunięte ze środowiska operacyjnego i nie można uzyskać do nich dostępu.	3.45

M16.12	Dzienniki dla urządzeń sieciowych w krytycznych funkcjach bezpieczeństwa muszą być w pełni rejestrowane i udostępniane do audytu przez 13 miesięcy.	3.56, 3.57
M16.21	Wskazania potencjalnej nietypowej aktywności są niezwłocznie oceniane, badane i rozwiązywane.	3.56, 3.57
M21.02	Środki podejmowane przez dostawcę zgodnie z Regulacją 3(3)(f) powinny zazwyczaj obejmować zapewnienie, w zakresie, w jakim jest to racjonalnie wykonalne, że sprzęt wykonujący funkcje nadzoru sieci dostawcy znajduje się w Wielkiej Brytanii i jest obsługiwany przez personel z siedzibą w Wielkiej Brytanii.	16.21
M21.03	Dostawca zachowa zdolność techniczną z siedzibą w Wielkiej Brytanii, aby zapewnić specjalistyczną wiedzę na temat działania sieci dostawcy w Wielkiej Brytanii i zagrożeń dla sieci dostawcy w Wielkiej Brytanii.	16.2, 16.20-16.22
M21.04	Jeśli dane są przechowywane za granicą, dostawca prowadzi wykaz lokalizacji, w których dane są przechowywane. Ryzyko związane z przechowywaniem danych w tych lokalizacjach, w tym wszelkie ryzyko związane z lokalnymi przepisami o ochronie danych, będzie zarządzane w ramach procesów zarządzania ryzykiem dostawcy.	3.8