Zasady dotyczące zdalnego dostępu VPN dla Wykonawcy

1. Podstawowe informacje
2. Zamawiający udostępni Wykonawcy zdalny dostęp do systemów teleinformatycznych zwany dalej Zdalnym dostępem.
3. Zdalny dostęp udostępniony zostanie na okres trwania Umowy.
4. Zdalny dostęp zostanie udostępniony wyłącznie wyznaczonym osobom.
5. Zdalny dostęp może zostać odebrany w szczególności w przypadku:
   1. Wygaśnięcia, rozwiązania lub wypowiedzenia Umowy,
   2. Korzystania ze Zdalnego dostępu przez osobę do tego nieupoważnioną,
   3. Wykrycia szkodliwego oprogramowania na urządzeniu korzystającym ze Zdalnego dostępu,
   4. Ujawnienia haseł dostępu lub innych danych uwierzytelniających,
   5. Wykorzystania łącza w sposób niezgodny z umową, w tym:
      1. Prób skanowania całych podsieci lub portów infrastruktury Zamawiającego,
      2. Wielokrotnych prób połączeń do serwerów w Internecie,
      3. Nawracających prób połączeń do sieci anonimizujących,
      4. Prób połączeń ze zidentyfikowanymi adresami Command and Control botnetów lub innymi adresami wskazującymi na infekcję po stronie Wykonawcy,
      5. Prób zestawienia nieautoryzowanych kanałów dostępu,
      6. Prób zestawienia połączeń do których dostęp nie został wskazany,
      7. Prób nadużycia przyznanych uprawnień,
   6. Nieprzestrzegania zasad bezpieczeństwa, które Zamawiający zawarł w Umowie.
6. Jeżeli po upływie 1 roku od udostępnienia konta użytkownikowi, koordynator umowy ze strony Zamawiającego nie złożył wniosku o jego przedłużenie na następny okres.
7. Odebranie Zdalnego dostępu z przyczyn opisanych w punkach od 4.2 do 4.6 traktowane jest jako odebranie Zdalnego dostępu z przyczyn leżących po stronie Wykonawcy.
8. Zamawiający zastrzega sobie możliwość rejestrowania wszystkich sesji Zdalnego dostępu nawiązywanych przez osobę upoważnioną po stronie Wykonawcy.
9. Przy pracy z kontami o uprawnieniach uprzywilejowanych, Zamawiający wymaga korzystania przez Wykonawcę ze Zdalnego dostępu poprzez system do zarządzania uprzywilejowanym dostępem (PAM/PIM) oraz stacje przesiadkowe. Bezpośredni dostęp do aplikacji jest zablokowany.
10. Wszelkie informacje dotyczące parametrów technicznych i technologicznych Zdalnego dostępu stanowią informację poufną i nie mogą być ujawniane osobom trzecim.
11. Dane uwierzytelniające stanowią informację poufną i powinny być znane wyłącznie użytkownikowi danego konta.
12. Wykonawca bez zbędnej zwłoki powiadomi Zamawiającego o każdym zauważonym przez niego zakresie Zdalnego dostępu, który jest nieadekwatny do zakresu uprawnień niezbędnych w celu realizacji Umowy.
13. Korzystanie ze zdalnego dostępu możliwe jest tylko przez klienta VPN wskazanego przez Zamawiającego.
14. Systemy informatyczne i zasoby teleinformatyczne udostępnione poprzez Zdalny dostęp mogą być wykorzystywane przez osoby uprawnione do korzystania ze Zdalnego dostępu wyłącznie zgodnie z ich przeznaczeniem, z należytą starannością oraz w takim stopniu, w jakim posiadają uprawnienia.
15. Zabronione jest korzystanie ze Zdalnego dostępu z komputerów dostępnych w miejscach publicznych, np. kawiarenki internetowe, kioski.
16. Zabronione jest korzystanie ze zdalnego dostępu w miejscach, w których zachodzi ryzyko ujawnienia informacji wyświetlanych na ekranie osobom postronnym, np. na dworcu kolejowym, w restauracji, itp.
17. Zabronione jest pozostawianie bez opieki komputera z aktywnym Zdalnym dostępem.
18. Zabronione jest instalowanie, odinstalowywanie oprogramowania i zmiana konfiguracji na serwerach Zamawiającego przez Wykonawcę bez wiedzy i zgody Zamawiającego.
19. Zabronione jest eksportowanie lub kopiowanie danych z Systemów informatycznych Zamawiającego bez zgody Zamawiającego.
20. Wymagania techniczne i organizacyjne
21. Wykonawca powinien posiadać wdrożoną politykę bezpieczeństwa informacji obejmującą świadczone na rzecz Zamawiającego usługi.
22. Sieć komputerowa, z której inicjowany jest Zdalny dostęp powinna być chroniona dedykowaną zaporą sieciową. Jeśli dostęp inicjowany jest bezpośrednio ze stacji roboczej np. przez modem to wymagany jest włączony firewall na tej stacji.
23. Wykonawca zobowiązany jest do zapewnienia bezpieczeństwa fizycznego urządzeń, z których następuje Zdalny dostęp.
24. Wykonawca jest zobowiązany, aby przez cały okres korzystania ze Zdalnego dostępu komputery oraz urządzenia mobilne, z których nawiązywane są połączenia:
    1. Posiadały system operacyjny Windows w wersji min 10 lub Linux z zainstalowanymi wszystkimi aktualizacjami krytycznymi oraz zaktualizowanym oprogramowaniem dodatkowym - jeżeli jest zainstalowane, w szczególności: przeglądarki internetowe, Adobe Reader, Java;
    2. Posiadały system operacyjny Android w wersji wspieranej przez producenta z zainstalowanymi wszystkimi aktualizacjami bezpieczeństwa.
    3. Posiadały zainstalowane oprogramowanie antywirusowe. Oprogramowanie antywirusowe musi być aktualizowane automatycznie przynajmniej raz dziennie i posiadać aktywną ochroną (skanowanie) w tle. Oprogramowanie antywirusowe musi w sposób automatyczny przeprowadzać pełne skanowanie systemu nie rzadziej niż raz w miesiącu (nie dotyczy urządzeń z system Android).
    4. Nie były wykorzystywane do udostępniania Zdalnego dostępu dalej na inne komputery lub urządzenia.
    5. Od momentu ustanowienia Zdalnego dostępu do jego zakończenia urządzenie nie może być wykorzystywane do innych celów niż związane z wykonywaniem Umowy.
    6. Dla komputerów wymagane jest oprogramowanie szyfrujące zawartość całego dysku twardego.
25. Wykonawca zapozna osoby, które wyznaczył do korzystania ze Zdalnego Dostępu, z wymaganiami technicznymi i organizacyjnymi opisanymi w niniejszym Załączniku i zobowiąże do ich stosowania.
26. W przypadku, kiedy pracownik Wykonawcy posiadający Zdalny dostęp VPN do systemu Zamawiającego zakończy świadczenie pracy na rzecz Wykonawcy lub też nie realizuje już poprzez Zdalny dostęp VPN prac na rzecz Zamawiającego, Wykonawca zobowiązany jest do niezwłocznego tj. nie później niż w ciągu 2 dni roboczych, wystąpienia do Zamawiającego z wnioskiem o odebranie uprawnień zdalnego dostępu VPN dla tego pracownika.
27. Każda osoba, po stronie Wykonawcy zanim uzyska dostęp VPN do zasobów Zamawiającego, ma obowiązek zapoznania się z zasadami Bezpieczeństwa Zamawiającego.
28. Udokumentowanie zapoznania się z w.w. zasadami bezpieczeństwa leży po stronie Wykonawcy, który odpowiada za działania osób które po jego stronie uzyskały dostęp jak za działania własne.
29. Prawo do kontroli
30. W związku z faktem, że Spółki Grupy TAURON pełnią rolę Operatora Usługi Kluczowej w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa Dz.U. 2018 poz. 1560 oraz ciążącym na nim ustawowym obowiązku w zakresie zapewnienia bezpieczeństwa własnej infrastruktury, Zamawiający ma prawo do kontroli spełniania wymagań bezpieczeństwa przez Wykonawcę. Zamawiający realizuje powyższy obowiązek poprzez:
    1. weryfikację sposobu użytkowania Zdalnego dostępu przez Wykonawcę   
       w sposób dopuszczony w Umowie;
    2. weryfikację sposobu użytkowania Zdalnego dostępu przez Wykonawcę poprzez przeprowadzanie inspekcji nagrywanych sesji, ruchu sieciowego;
    3. weryfikację spełnienia wymagań technicznych w stosunku do podłączanych stacji roboczych z których świadczona jest umowa serwisowa;
    4. weryfikację posiadania i stosowania polityki bezpieczeństwa informacji przez Wykonawcę, zgodnie z punktem II podpunkt 1.
31. Ze względu na ciążący na Zamawiającym obowiązek kontroli bezpieczeństwa Wykonawca, udzieli Zamawiającemu wszelkich informacji niezbędnych do wypełnienia tego obowiązku w terminie 3 dni roboczych od dnia dostarczenia Wykonawcy żądania wyjaśnień, za wyjątkiem sytuacji opisanej w punkcie III.
32. Po zakończeniu kontroli, o której mowa w ust. 1 powyżej, przedstawiciel Zamawiającego sporządza protokół zawierający wyniki kontroli i przedstawia go Wykonawcy.
33. Zamawiający może sformułować zalecenia pokontrolne i żądać ich wykonania, o ile są zgodne z Umową, oraz określić termin ich realizacji.