Wymagania dotyczące zgłaszania i obsługi incydentów bezpieczeństwa

1. Zgłaszanie incydentów bezpieczeństwa
2. Wykonawca zobowiązany jest do bezzwłocznego informowania Zamawiającego o:
   1. zauważonym przypadku naruszenia bezpieczeństwa systemów i zasobów teleinformatycznych,
   2. odnalezieniu podatności lub luki w zabezpieczeniach,
   3. stwierdzonym przypadku naruszenia integralności sprzętu, oprogramowania bądź podejrzeniu próby takiego naruszenia,
   4. stwierdzonym przypadku infekcji szkodliwym oprogramowaniem stacji roboczej, z której inicjowany jest Zdalny dostęp,
   5. podejrzeniu utraty poufności indywidualnych danych uwierzytelniających,
   6. wykrytych incydentach bezpieczeństwa dot. danych powierzonych do przetwarzania przez Grupę TAURON (np. wielokrotne nieudane próby logowania, lub wykrycie złośliwej zawartości) oraz o ataku na systemy innych klientów Wykonawcy na infrastrukturze wspólnej z Zamawiającym.
3. 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.
4. Wykonawca bez zbędnej zwłoki zobowiązany jest do poinformowania Zamawiającego o każdym zaistniałym incydencie IT związanym pośrednio lub bezpośrednio ze Zdalnym dostępem, lub mogącym mieć wpływ na systemy/zasoby.
5. Wykonawca zobowiązuje się do informowania Zamawiającego o wykrytych incydentach bezpieczeństwa dot. danych powierzonych do przetwarzania przez Grupę TAURON (np. wielokrotne nieudane próby logowania, lub wykrycie złośliwej zawartości) oraz o ataku na systemy innych Wykonawcy na infrastrukturze połączonej z Zamawiającym.
6. Zgłaszanie incydentów bezpieczeństwa powinno zostać dostarczone na dedykowany adres e–mail w ciągu 24h od wykrycia incydentu.
7. Do zgłaszania incydentów bezpieczeństwa wykrytych przez Zamawiającego lub wykrytych przez Wykonawcę ustala się następujące dane kontaktowe:

Ze strony Zamawiającego: Ze strony Wykonawcy:

adres e-mail: [cuwit@tauron.pl](mailto:cuwit@tauron.pl) adres e-mail:……….………………………………

nr telefonu: +48 500 99 5555 nr telefonu:……….……………………………….

Dane te mogą być skutecznie zmieniane za pisemnym powiadomieniem drugiej strony (pod rygorem nieważności).

1. Obsługa incydentów bezpieczeństwa

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 nich ustawowym obowiązku zgłaszania incydentów bezpieczeństwa do krajowych CSIRT-ów w ramach Krajowego Systemu Cyberbezpieczeństwa, Wykonawca powinien w przypadku wystąpienia incydentu bezpieczeństwa:

1. zapewnić pomoc i przekazać wszelkie dalsze informacje dotyczące tego Incydentu Zamawiającemu oraz służbom SOC Grupy TAURON,
2. zapewnić pomoc w ustaleniu przyczyn incydentu bezpieczeństwa,
3. umożliwić Zamawiającemu uczestnictwo w czynnościach podejmowanych w celu wyjaśnienia przyczyny Incydentu, jeżeli zachodzi potrzeba,
4. podjąć niezwłocznie wszelkie czynności mające na celu usunięcie negatywnych skutków incydentu bezpieczeństwa oraz wdrożyć zabezpieczenia zapobiegające ponownemu wystąpieniu incydentów bezpieczeństwa. Podejmowane działania powinny być uzgodnione z Zamawiającym.
5. zebrać wszystkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności wystąpienia Incydentu i przeciwdziałaniu podobnym Incydentom w przyszłości i w tym celu współpracować z Zamawiającym na każdym etapie wyjaśniania sprawy.