Wymogi IT dla kontrahentów

Poniższe wymagania mają zastosowanie do wszelkich produktów i usług IT takich jak sprzęt komputerowy (w tym maszyny przemysłowe posiadające system operacyjny), aplikacje, hosting itp.

1. Odpowiedzialnością Dostawcy jest zapewnienie zgodności towaru i/lub usługi z obowiązującą polityką bezpieczeństwa UTC wg informacji zawartych w tym dokumencie oraz innych informacji przekazanych przez dział IT PWRZ.

2. Dostarczany sprzęt komputerowy:

· preferowana konfiguracja serwerów, komputerów typu desktop, laptopów lub innych urządzeń komputerowych zgodna z obowiązującym aktualnie standardem PWRZ (informacja dostępna na bieżąco do wglądu w dziale IT PWRZ);
· preferowany system operacyjny zgodny z obecnym standardem PWRZ (informacja dostępna na bieżąco do wglądu w dziale IT PWRZ);
· Dostawca zobowiązany jest dostarczyć potwierdzenie legalności (certyfikat licencyjny, faktura) na każde zainstalowane i/lub dostarczone oprogramowanie;
· warunki gwarancji i serwisowania dostarczanego sprzętu komputerowego muszą być jasno zdefiniowane przez Dostawcę;
· Dostawca nie jest upoważniony do wywożenia dysków twardych i/lub innych nośników informacji wykorzystywanych w celach testowych i/lub produkcyjnych (w dostarczonym systemie) poza teren przedsiębiorstwa PWRZ bez wcześniejszej, pisemnej zgody PWRZ IT.

3. Zakres uprawnień na dostarczanym sprzęcie komputerowym:

· Dostawca posiada prawo do konfiguracji sprzętu komputerowego jedynie przed odbiorem końcowym tego sprzętu; uprawnienia do wykonywania czynności serwisowych, konfiguracyjnych i innych po uruchomieniu maszyny lub aplikacji muszą być zatwierdzone przez dział IT PWRZ;
· podczas odbioru końcowego urządzenia/projektu itp. Dostawca zobowiązany jest przekazać wszystkie prawa, hasła dostępu itp. do systemów, kont oraz aplikacji dostarczanych w ramach realizacji Umowy;
· hasła dostępu należy przekazać w formie pisemnej pracownikowi działu IT PWRZ;
· Dostawca nie ma możliwości uzyskać praw użytkownika uprzywilejowanego (konta typu administrator, root, itp.) na dostarczanym sprzęcie komputerowym w trakcie jego użytkowania w procesie produkcyjnym. Uprawnienia takie mogą być nadane wyłącznie za zgodą działu IT PWRZ w uzasadnionym przypadku potrzeby wykonania usługi serwisowej, konfiguracyjnej lub innej.

4. Łączenie zdalne do systemów komputerowych PWRZ jest możliwe wyłącznie przy spełnieniu następujących warunków:

· Dostawca złoży pisemne poświadczenie o akceptacji warunków umowy o ochronę informacji, która jest wymagana przed rozpoczęciem współpracy;

· Dostawca oświadcza, zapewnia, zobowiązuje się i wyraża zgodę, iż możliwość dostępu zdalnego do systemów komputerowych PWRZ zostaje udzielona na czas nie dłuższy, niż okres realizacji Umowy;
· Dostawca zobowiązuje się do spełniania przepisów kontroli eksportu mających zastosowanie do przekazywanych danych (jeśli dane tego wymagają).
· Dostawca potwierdza, że w przypadku połączenia zdalnego korzysta z bezpiecznych kanałów komunikacji;

5. PWRZ zastrzega sobie prawo odmowy dostępu pracowników Dostawcy do systemu informatycznego PWRZ, podłączenia modemu i/lub karty sieciowej do sieci zewnętrznej, łącza zewnętrznego, linii telefonicznej itp. jeśli powyższe warunki nie są spełnione.

6. Jeżeli przedmiotem Umowy jest aplikacja opracowana na potrzeby PWRZ to kody źródłowe użyte do jej opracowania stają się własnością PWRZ. Dostawca zobowiązany jest przekazać kody źródłowe aplikacji tworzonych na rzecz PWRZ. PWRZ posiada prawa do użytkowania, tworzenia kopii oraz modyfikowania dostarczanych kodów źródłowych.

7. Dostawca gwarantuje, że posiada odpowiednie prawa własności do narzędzi oraz oprogramowania, przy użyciu których zostały wytworzone towary i/lub usługi na rzecz PWRZ będące przedmiotem Umowy.

8. Dostawca pokrywa wszystkie koszty związane z odszkodowaniami i/lub karami, w przypadku, gdy sposób tworzenia towaru i/lub usługi naruszy prawo własności innych podmiotów.

9. Jeśli elementem umowy jest tworzenie i/lub modyfikowanie serwisu WWW, wówczas:

· zawartość umieszczona na stronie WWW jest chroniona przez prawo autorskie; prawa te należą do PWRZ. Implementowanie i wykorzystywanie narzędzi służących do wyszukiwania treści musi być zgodne z polityką UTC. Jeśli narzędzia służące do wyszukiwania treści tworzą kopie danych źródłowych, wówczas kopie te podlegają takiej samej ochronie jak dane źródłowe;
· Dostawca zapewni regularne aktualizacje strony WWW zawierającej dane PWRZ poprzez interfejs elektroniczny. Za określenie zakresu danych i częstotliwość aktualizacji odpowiedzialne jest PWRZ.

10. Wszystkie aplikacje muszą wykorzystywać narzędzia autoryzacji i kontroli dostępu lub aplikacje te muszą mieć zaimplementowaną funkcjonalność zapewniającą bezpieczeństwo i zgodność z polityką bezpieczeństwa UTC, a w tym między innymi:

· hasła dostępu do systemów muszą być odpowiednio trudne do złamania; system nie powinien przyjmować zbyt łatwych haseł jak np. wyrazów podobnych do posiadanego identyfikatora, uporządkowanych ciągów znaków z klawiatury (np. 123456, asdfgh) powszechnie znanych akronimów itp.;
· system powinien mieć możliwość wymuszenia, aby hasła miały co najmniej 8 znaków oraz były zmieniane przynajmniej raz na 60 dni;

· hasła muszą być złożone (tzn. składać się ze znaków z co najmniej trzech wymienionych grup: małe litery, duże litery, cyfry, znaki specjalne)
· dla kont serwisowych i komunikacyjnych (tzw. service ID) hasła muszą składać się z co najmniej 15 znaków;
· minimalny okres życia hasła to 1 dzień; hasła powinny być dozwolone do użycia powtórnie dopiero po 6-ciu miesiącach lub powinno być pamiętane i zablokowane do powtórnego użycia przynajmniej 5 ostatnich haseł;
· hasła nie mogą być wyświetlane ani przechowywane w jakimkolwiek pliku w postaci niezaszyfrowanej;
· system powinien być tak skonfigurowany, aby konta użytkowników, na które nie było logowania przez okres trzech miesięcy były automatycznie blokowane; po max 12 miesiącach braku aktywności konta użytkowników będą ręcznie usuwane

11. Ochrona danych PWRZ w systemach Dostawcy:

· Jeśli w ramach Umowy Dostawca otrzymuje a następnie przechowuje i/lub przetwarza wrażliwe dane PWRZ (jak np. dane osobowe, finansowe, dane techniczne jak np. rysunki, technologie itp.), wówczas Dostawca musi dostarczyć kopię aktualnej polityki bezpieczeństwa dotyczącej przechowywania i przetwarzania danych oraz politykę dotyczącą fizycznego dostępu do urządzeń, na których są przechowywane i/lub przetwarzane dane PWRZ. Dostawca powinien raz na rok dostarczać PWRZ aktualną politykę bezpieczeństwa.
· Wymaga się, aby Dostawca wydzielił przekazane dane PWRZ i przechowywał w oddzielnych bazach danych, do których dostęp ma jedynie PWRZ, uprawnione strony oraz autoryzowani pracownicy Dostawcy, odpowiedzialni za utrzymanie danego środowiska.
· Dostawca zobowiązuje się, że dostęp do danych PWRZ będzie ograniczony wyłącznie do osób niekaranych.
· Dostawca jest odpowiedzialny za zapewnienie ochrony przed nieautoryzowanym dostępem do przechowywanych w systemach Dostawcy danych PWRZ.
· Wobec danych PWRZ muszą być przez cały okres realizacji Umowy wykonywane kopie bezpieczeństwa. Minimalne wymogi to backup przyrostowy, realizowany co 24 godziny oraz pełen backup, wykonywany co 7 dni. Okres przechowywania kopii bezpieczeństwa to minimum 30 dni.
· PWRZ lub strona trzecia wskazana przez PWRZ ma prawo przeprowadzić audit bezpieczeństwa w obiekcie Dostawcy bez wcześniejszego powiadamiania Dostawcy. Jeśli dane PWRZ są przechowywane w środowisku współdzielonym, PWRZ może powołać się na stronę trzecią, aby przeprowadziła taki audit. Audit może uwzględniać wszystkie obiekty oraz urządzenia, na których przechowywane są dane PWRZ, włączając w to kopie bezpieczeństwa tych danych, a także może obejmować weryfikację, czy wszystkie niezbędne kontrole są prowadzone u Dostawcy zgodnie z polityką bezpieczeństwa UTC.
· Niepowodzenie przebiegu auditu bezpieczeństwa i/lub ochrony informacji określonych w niniejszych wymaganiach u Dostawcy może być podstawą do rozwiązania Umowy z Dostawcą. PWRZ może wskazać na „słabe punkty" Dostawcy, natomiast Dostawca powinien w ciągu 30 dni dostarczyć PWRZ plan usunięcia tych nieprawidłowości i jeśli PWRZ sobie tego zażyczy Dostawca powinien zastosować rozwiązania tymczasowe do momentu usunięcia wszelkich nieprawidłowości. Jeśli ryzyka zidentyfikowane przez

PWRZ nie zostaną usunięte w ciągu zadanego czasu lub jeśli Dostawca odmówi usunięcia nieprawidłowości, wówczas PWRZ może rozwiązać Umowę ze skutkiem natychmiastowym.
· Zgodnie z polityką bezpieczeństwa UTC, wrażliwe dane PWRZ muszą być szyfrowane w przypadku przesyłania ich poprzez sieci publiczne takie jak np. Internet. Zastosowane technologie szyfrowania muszą zostać zatwierdzone przez dział IT PWRZ i być zgodne z obowiązującymi przepisami prawa. Dostawca akceptuje fakt, że dane wrażliwe będą ze strony PWRZ przekazywane w formie zaszyfrowanej w przypadku przesyłania ich np. pocztą elektroniczną, zgodnie z obowiązującym standardem szyfrowania UTC.
· Przed lub w momencie podpisania Umowy Dostawca musi przedstawić PWRZ plan, który opisuje sposób przekazania do PWRZ wszelkich posiadanych i przechowywanych przez Dostawcę danych PWRZ, włączając w to kopie bezpieczeństwa i dane archiwalne, a także sposób trwałego usunięcia tych danych z systemu Dostawcy w przypadku zakończenia Umowy. Plan ten musi uwzględniać przekazanie danych do PWRZ w postaci zgodnej ze standardem oprogramowania PWRZ, w przeciwnym wypadku Dostawca zobowiązany jest dostarczyć licencję na odpowiednie oprogramowanie umożliwiające korzystanie i odtworzenie przekazanych danych.
· Dostawca potwierdza, że posiada procedury i zabezpieczenia przeciwko znanym zagrożeniom bezpieczeństwa danych (np. stosuje i regularnie aktualizuje oprogramowanie AV, jest zdolny do wykrywania włamań i prób włamań do swoich systemów komputerowych itp);· Dostawca zobowiązany jest powiadomić PWRZ o jakichkolwiek próbach dotyczących pozyskania informacji PWRZ przez strony trzecie i/lub włamaniach lub próbach włamań do systemów informatycznych Dostawcy.

12. Dostawca zobowiązany jest zapewnić aktualizację swoich procedur w przypadku zmian w polityce bezpieczeństwa UTC, tak, aby zapewnić zgodność z tą polityką.

13. Każdy zewnętrzny użytkownik musi postępować zgodnie z wymogami polityk bezpieczeństwa i standardów PWRZ/UTC. Dostawca jest zobowiązany realizować program podnoszenia świadomości odnośnie bezpieczeństwa

14. PWRZ pozostawia sobie prawo do oceny możliwości spełnienia wymogów polityki bezpieczeństwa UTC przez Dostawcę. Dostawca ma obowiązek przedstawić na żądanie PWRZ pisemne oświadczenie, w jaki sposób powyższe wymagania są spełnione.