URZĄD MIASTA ŁODZI

Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia

Kod CPV – 48761000-0 Pakiety oprogramowania antywirusowego

1. Przedmiotem niniejszego postępowania jest dostawa oprogramowania antywirusowego wraz z asystą techniczną na okres 12 miesięcy (liczony jednak nie wcześniej niż od 16 maja 2021 r.), obejmująca wykorzystanie oprogramowania na 4000 stacjach roboczych, serwerach i urządzeniach mobilnych oraz przez 4 500 użytkowników bramki pocztowej (bramki smtp).

2. Termin wykonania zamówienia

Wykonawca wykona zamówienie w niżej wymienionych etapach:

Etap I:

a. Wykonawca dostarczy oprogramowanie wraz z licencjami do siedziby Zamawiającego w terminie do 22 dni roboczych od daty wejścia w życie umowy określonej w § 12 ust. 4, jednak nie wcześniej niż przed datą wdrożenia i uruchomienia oprogramowania.

b. Potwierdzeniem dostarczenia oprogramowania wraz z licencjami będzie podpisanie bez zastrzeżeń, przez upoważnionych przedstawicieli Stron protokołu zdawczo-odbiorczego.

c. Wykonawca wdroży pełną funkcjonalność oprogramowania antywirusowego w terminie do 22 dni roboczych od daty wejścia w życie umowy określonej w § 12 ust. 4.

d. Potwierdzeniem wdrożenia i uruchomienia oprogramowania będzie podpisanie bez zastrzeżeń, przez upoważnionych przedstawicieli Stron protokołu wdrożenia. Strony ustalają, że datą uruchomienia oprogramowania jest data podpisania protokołu wdrożenia.

Etap II:

a. Gwarancja i asysta techniczna wdrożonego oprogramowania przez okres 12 miesięcy od dnia wdrożenia i uruchomienia oprogramowania.

Oferowane rozwiązanie musi spełniać wymagania opisane w niniejszym opisie przedmiotu zamówienia w pkt. I. - *„Wymagania minimalne dotyczące rozwiązania”* oraz w pkt. II - *„Wymagania minimalne dotyczące wdrożenia”*.

Zamawiający używa obecnie oprogramowanie Kaspersky Endpoint Security for Bussines Advanced – 4000 szt. licencji, oraz Kaspersky Secure Mail Gateway – 2800 szt. licencji z terminem wygaśnięcia 16 maja 2021 r.

URZĄD MIASTA ŁODZI

I. Wymagania minimalne dotyczące rozwiązania

1. Wymagania ogólne

1. Rozwiązanie musi zapewnić ochronę w dwóch obszarach tj. ochronę stacji końcowej użytkownika i serwerów oraz ochronę poczty smtp (instalowane osobno, nie na działającym serwerze pocztowym).
2. Wszystkie moduły oprogramowania w każdym z obszarów opisanych w pkt. 1) muszą posiadać konsolę zarządzającą. Jedna konsola musi obejmować co najmniej funkcjonalność ochrony stacji końcowej użytkownika oraz serwerów. Zarządzanie systemem ochrony poczty smtp może być realizowane z wykorzystaniem konsoli dedykowanej lub poprzez konsolę do zarządzania ochroną stacji końcowej użytkownika oraz serwerów.
3. Zamawiający nie dopuszcza rozwiązań typu Unified Threat Managment (UTM).
4. W obszarze ochrony stacji końcowej użytkownika oraz serwerów, oprogramowanie musi realizować co najmniej następujące funkcjonalności: ochrona antywirusowa, firewall, ids/ips na interfejsie sieciowym, kontrola aplikacji na stacjach roboczych i serwerach. Szczegółowy opis funkcjonalności jest opisany w pkt. 2. „Szczegółowe wymagania techniczne". Ponadto musi koegzystować i nie zakłócać jednocześnie działania aplikacji Palo Alto Networks Traps.
5. W obszarze ochrony poczty smtp oprogramowanie musi realizować co najmniej następujące funkcjonalności: ochronę antywirusową i antyspamową. Szczegółowy opis funkcjonalności jest opisany w pkt. 2. „Szczegółowe wymagania techniczne".
6. Pełna funkcjonalność klienta dla stacji roboczej musi być zawarta w jednym pliku instalacyjnym msi, zgodnym z Windows Installer.
7. Oprogramowanie musi działać na systemach Windows 7 z SP1, wszystkie wersje Windows: 8.x, 10 , Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019
8. Dla urządzeń mobilnych oprogramowanie musi działać na systemie Android i IOS.
9. Oferowane rozwiązanie musi poprawnie funkcjonować w zakresie serwerów zarządzających (konsola zarządzająca) oraz ochrony serwerów smtp w środowisku Microsoft Hyper-V 2016 i 2019.
10. Komponenty rozwiązania, które realizują funkcjonalności takie jak: firewall, zapobieganie włamaniom i kontrola aplikacji na stacjach roboczych, muszą działać na wszystkich powyższych platformach 32 i 64-bitowych.
11. Serwer zarządzający musi działać na systemach Windows Server: 2016 i 2019
12. Zarządzanie systemem ma być zapewnione poprzez graficzną konsolę administratora.
13. Rozwiązanie ma zapewniać skalowalność (obsługa min. 5 000 stacji).

14. Komunikacja pomiędzy agentami i serwerem ma być szyfrowana i kompresowana.
15. Numery portów używane do komunikacji mają mieć możliwość konfiguracji.
16. Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.
17. Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego źródła aktualizacji z możliwością konfiguracji określenia prędkości ich pobierania z serwera zarządzającego.
18. Jeżeli rozwiązanie wykorzystuje oprogramowanie firm trzecich, muszą zostać dostarczone wszelkie licencje na ich używanie.
19. Asysta techniczna świadczona przez producenta w swoim zakresie musi obejmować upgrade oprogramowania i jego składników, update definicji antywirusowych i antyspamowych oraz pomoc techniczną przy rozwiązywaniu problemów z zaoferowanym oprogramowaniem. Czas naprawy nie dłuższy niż 14 dni.

2. Szczegółowe wymagania techniczne.

1. Ochrona antywirusowa stacji roboczej oraz serwerów:

a. Usuwanie wirusów, makro–wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware” i „adware”, włącznie z usuwaniem zmian wprowadzonych do systemu przez oprogramowanie tego typu;
b. Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym;
c. Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta za zaufane;
d. Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych;
e. Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane: na dyskach twardych, w boot sektorach, na dyskietkach, na płytach CD/DVD, na zewnętrznych dyskach twardych (np. podłączonych przez port USB);
f. Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej;
g. Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.
h. Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych.

URZĄD MIASTA ŁODZI

i. Aktualizacja definicji wirusów nie wymagająca zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej;
j. Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące;
k. Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zestawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów;
l. Możliwość natychmiastowego „wypchnięcia" definicji wirusów do stacji klienckich;
m. Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 2 razy dziennie;
n. Możliwość aktualizacji bazy definicji wirusów średnio co 1 godzinę;
o. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów;
p. Moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger;
q. Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe;
r. Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione;
s. Skanowanie poczty klienckiej (na komputerze klienckim);
t. Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach;
u. W wypadku systemu Windows 8 i 10, wsparcie dla funkcji ELAM (Early Launch Anti-Malware).

2. Firewall dla stacji roboczej oraz serwerów

a. Pełne zabezpieczenie stacji klienckich przed nieautoryzowanymi próbami dostępu do komputerów;
b. Moduł firewall ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe;
c. Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać;
d. Administrator może konfigurować dostęp stacji do następujących protokołów TCP, UDP, ICMP, IGMP
e. Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane jako: całkowicie bezpieczne lub niebezpieczne;

URZĄD MIASTA ŁODZI

f. Program musi wykrywać próby wyszukiwania luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli;
g. Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: protokół sieciowy, stacja docelowa, aplikacja
h. Domyślne reguły zezwalające na ruch DHCP, DNS, WINS;
i. Wsparcie dla protokołu IPv6;
j. Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www – **funkcjonalność opcjonalna, dodatkowo punktowana**.

3.IDS/IPS na interfejsie sieciowym dla stacji roboczych i serwerów

a. Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą;
b. Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC);
c. Wykrywanie trojanów i generowanego przez nie ruchu;
d. Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie;
e. Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków;

4.Kontrola aplikacji na stacjach końcowych oraz serwerach

a. Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji;
b. Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową;
c. Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym;
d. Produkt ma kontrolować dostęp do rejestru systemowego;
e. Możliwość utworzenie listy zaufanych aplikacji (tzw. białej listy) i konfiguracji produktu w taki sposób, aby żadna inna aplikacja/biblioteka spoza listy nie mogła uruchomić się na komputerze;
f. Możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, aby tylko aplikacje znajdujące się na liście nie mogły uruchomić się na komputerze;
g. Produkt ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne – **funkcjonalność opcjonalna, dodatkowo punktowana**;
h. Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych – **funkcjonalność opcjonalna, dodatkowo punktowana**.

URZĄD MIASTA ŁODZI

5.Szyfrowanie i deszyfrowanie na stacjach roboczych – funkcjonalność opcjonalna, dodatkowo punktowana.

a. Plików i katalogów
b. Całych dysków twardych
c. Przy użyciu algorytmu AES
d. Wszystkie działania związane z szyfrowaniem i deszyfrowaniem mają być całkowicie niewidoczne dla użytkownika
e. Mechanizm telefonicznego odzyskiwania hasła dla użytkownika znajdującego się poza siedzibą Zamawiającego

6.Centralna konsola zarządzająca dla stacji roboczych i serwerów

a. Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli;
b. Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci;
c. Produkt ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień;
d. Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym;
e. Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych;
f. Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu;
g. Uwierzytelnianie administratorów ma się odbywać z użyciem Microsoft Active Directory.
h. Dostęp do interfejsu produktu dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej;
i. Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta;
j. Lokalizacja ma być określana według istnienia lub nieistnienia: adresu IP, zakresu podsieci, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS;
k. Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji;
l. W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji innych produktów bezpieczeństwa, która uruchomi się automatycznie przed instalacją produktu;
m. Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym;
n. Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej;

URZĄD MIASTA ŁODZI

o. Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia: dostępności nowego oprogramowania, pojawienia się nowego komputera, zdarzeń powiązanych z infekcjami wirusów, stanu serwerów zarządzających;

p. Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

q. Możliwość przejęcia stacji roboczej za pomocą konsoli administracyjnej.

7.Ochrona antywirusowa, antyspamowa oraz filtrowanie treści dla serwerów poczty smtp

a. licencja pozwalająca uruchomić zaoferowane rozwiązanie w środowisku wirtualnym Hyper-V;

b. Integracja z LDAP;

c. Zintegrowane rozwiązanie antywirusowe, antyspamowe i filtrowania treści;

d. Praca, jako bramka pocztowa;

e. Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowania na serwer usługodawcy;

f. Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów lub dodanie wpisów na listach DNSBL i SURBL;

g. System ma zapewnić routing wiadomości pocztowych w oparciu o domenę i adres odbiorcy;

h. Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie się zawsze odbywać;

i. Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze blokowana;

j. Skaner antywirusowy ma skanować skompresowane załączniki do 10 poziomów zagnieżdżeń w głąb i ma być odporna na złośliwie spreparowane załączniki („załączniki spakowane zawierające złośliwe oprogramowanie”);

k. Wiadomości z wirusami typu mass-mailer mają być w całości odrzucane, bez podejmowania dodatkowych akcji takich jak np. powiadomienie;

l. Wykrywanie fałszywych URL-i w wiadomościach;

m. Nakładanie polityk na załączniki w oparciu o ich rozmiar, typ MIME lub jego rozszerzenie;

n. Wiadomości sklasyfikowane jako spam można: usunąć/odrzucić, dodać nagłówek wiadomości, zarchiwizować, dostarczyć bez modyfikacji;

o. Administrator ma mieć możliwość ingerencji w czułość rozwiązania;

p. Komunikacja w celu zarządzania systemem ma być szyfrowana;

q. System ma umożliwiać ustalenie co stało się z wiadomością;

r. System ma umożliwiać zapytanie o adres IP do globalnej bazy reputacji;

s. System musi wspierać autentykację SMTP;

URZĄD MIASTA ŁODZI

t. Wsparcie dla Transport Layer Security (TLS) – definiowane per domena lub polityka, Sender Policy Framework (SPF), Sender ID – funkcjonalność opcjonalna, dodatkowo punktowana.

II. Wymagania minimalne dotyczące wdrożenia.

1. Czas wdrożenia nowego systemu antywirusowego musi zakończyć się najpóźniej w 22 dniu roboczym od daty wejścia w życie umowy, podczas którego muszą zostać wykonane wszystkie niżej wymienione zadania.

a. Wykonawca najpóźniej do 5 dnia roboczego od daty podpisania umowy przedstawi projekt wdrożenia nowego systemu.

b. Zamawiający w ciągu kolejnych 2 dni roboczych dokona przeglądu projektu wdrożenia i przedstawi swoje uwagi i komentarze.

c. Wykonawca w ciągu kolejnych 2 dni roboczych uwzględni uwagi Zamawiającego i przedstawi nową wersję projektu wdrożenia.

d. Wykonawca w ciągu kolejnych 10 dni, wdroży pełną funkcjonalność systemu antywirusowego i zgłosi gotowość do odbioru.

e. Zamawiający w ciągu kolejnych 3 dni roboczych dokona odbioru systemu.

2. Instalacja systemu antywirusowego wraz z agentami może rozpocząć się dopiero, po zaakceptowaniu przez Zamawiającego projektu wdrożenia

3. Zakończenie wdrożenia systemu antywirusowego zostanie potwierdzone przez Zamawiającego i Wykonawcę poprzez podpisanie protokołu zdawczo-odbiorczego wdrożenia.

4. Wszystkie prace (poza wyszczególnionymi), które będą wykonywane u Zamawiającego muszą być realizowane w godzinach pracy Zamawiającego.

5. Wykonawca dokona analizy wykorzystywanego przez Zamawiającego systemu antywirusowego Kaspersky Endpoint Security for Bussines Advanced. Analiza musi obejmować minimum: architekturę funkcjonalną wdrożonego systemu, lokalizację wszystkich klientów oraz ich liczbę, systemy operacyjne, na których funkcjonują agenci. Analiza ta zostanie wykorzystana do odtworzenia wszystkich obecnie wdrożonych funkcjonalności i polityk bezpieczeństwa w zaoferowanym rozwiązaniu.

6. Wykonawca dokona deinstalacji obecnie wykorzystywanego systemu antywirusowego ochrony na wszystkich serwerach i wszystkich stacjach roboczych, o ile jest wymagana. W przypadku wystąpienia problemów podczas deinstalacji, ich rozwiązanie będzie należeć do Wykonawcy. Jednocześnie musi zostać zachowana pełna i prawidłowa funkcjonalność zainstalowanych innych aplikacji i systemów na danej stacji roboczej lub serwerze.

7. Wykonawca dokona instalacji agentów systemu antywirusowego na wszystkich stacjach roboczych podanych przez Zamawiającego. W przypadku wystąpienia problemów podczas instalacji, ich rozwiązanie będzie należeć do Wykonawcy. Jednocześnie musi zostać zachowana pełna i prawidłowa funkcjonalność zainstalowanych innych aplikacji i systemów na danej stacji roboczej.

URZĄD MIASTA ŁODZI

8. Terminy instalacji agentów systemu na stacjach roboczych i serwerach muszą zostać uzgodnione z Zamawiającym i przedstawione w postaci harmonogramu w projekcie wdrożenia.
9. Wykonawca dokona instalacji agentów systemu na serwerach pod nadzorem osób wyznaczonych przez Zamawiającego. W przypadku wystąpienia problemów podczas instalacji, ich rozwiązanie będzie należeć do Wykonawcy. Jednocześnie musi zostać zachowana pełna i prawidłowa funkcjonalność zainstalowanych innych aplikacji i systemów na danym serwerze.
10. Instalacje na serwerach wykonywane w godzinach pracy urzędu muszą zostać przeprowadzone w sposób, który nie zakłóca pracy użytkowników systemów pracujących na tych serwerach, w innym przypadku instalacja musi zostać przeprowadzona wyłącznie poza godzinami pracy.
11. W Urzędzie Miasta Łodzi stacje robocze zlokalizowane są w ok. 80 lokalizacjach na terenie miasta Łodzi. Lokalizacje w których sumaryczna ilość komputerów to ok. 3600 szt. podłączona jest siecią LAN o przepustowości min. 1Gbit/s, pozostałe to połączenia symetryczne 100Mbit/s oraz 2 połączenia 5Mbit/s (w sumie ok. 20-30 stacji roboczych).
12. Komputery podłączone są do Active Directory.
13. Obecnie wykorzystywane rozwiązanie musi funkcjonować do czasu pełnego wdrożenia zaoferowanego rozwiązania. W związku z tym, nie będzie możliwe wykorzystanie obecnie dedykowanych serwerów zarządzających dla nowego rozwiązania.
14. Zamawiający posiada infrastrukturę serwerową, która umożliwia uruchomienie w środowisku wirtualnym, 2 serwerów. Serwery mogą być utworzone na platformie Microsoft Hyper-v 2016 i środowisku zarządzającym SCVMM, każdy o następujących parametrach:

a. Maksymalna wielkość pamięci RAM - 12 GB.
b. Maksymalna wielkość przestrzeni dyskowej - 150 GB.
c. Maksymalna ilość VCPU – 4 szt.

15. Wykonawca przeprowadzi szkolenie dla min 10 osób w zakresie zarządzania systemem. Szkolenie musi zostać przeprowadzone zgodnie z zaleceniami dotyczącymi szkoleń, w zakresie czasu i tematyki zalecanej przez producenta zaoferowanego rozwiązania. Szkolenie musi być przeprowadzone nieodpłatnie na terenie miasta Łodzi lub poprzez Internet z aktywną komunikacją zarówno video jak i głosową z instruktorem prowadzącym szkolenie.
16. Wykonawca przygotuje dokumentację powykonawczą, która będzie obejmować, zawierającą w szczególności:

a. Analizę obecnie wykorzystywanego przez Zamawiającego systemu Kaspersky Endpoint Security for Bussines Advanced.
b. Architekturę wdrożonego systemu.
c. Wdrożone polityki.

URZĄD MIASTA ŁODZI

d. Procedury backupu i odtwarzania
e. Opis konfiguracji bramki smtp.
f. Procedury rekonfiguracji bramki smtp.
g. Procedury restartu systemu.

17. W przypadku wypowiedzenia lub zerwania umowy w trakcie realizacji procesu wdrożenia, Wykonawca zobowiązany jest wykonać wszystkie czynności na własny koszt, które przywrócą środowisko informatyczne Zamawiającego do stanu przed rozpoczęciem procesu wdrożenia. W przypadku, gdy Wykonawca nie wykona tych czynności, Zamawiający wykona niezbędne prace z wykorzystaniem firm trzecich a kosztami tych prac obciąży Wykonawcę.