

**UMOWA RAMOWA NA DOSTAWĘ URZĄDZEŃ WIELOFUNKCYJNYCH WRAZ Z ICH
INSTALACJĄ ORAZ DOSTAWĄ OPROGRAMOWANIA NR**

zawarta w Warszawie, w dniu [***] r. *[lub wariantowo jeżeli umowa jest podpisywana kwalifikowanym podpisem elektronicznym:] w dniu podpisania przez ostatnią ze Stron,* pomiędzy:

Polską Spółką Gazownictwa sp. z o.o. z siedzibą w Tarnowie, ul. Wojciecha Bandrowskiego 16, 33-100 Tarnów, Oddział Wsparcia w Warszawie, adres: ul. Krucza 6/14, 00-537 Warszawa, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000374001, NIP 5252496411, REGON 142739519, o kapitale zakładowym 10.687.868.000,00 zł, którą reprezentuje:

Pełnomocnicy, na podstawie załączonego do umowy pełnomocnictwa,

zwaną dalej „**Zamawiającym**”

a

_____ z siedzibą w _____, ul. _____, _____, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy _____, Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS _____, NIP _____, REGON _____, o kapitale zakładowym _____, którą reprezentuje:

1. _____ – _____,
2. _____ – _____,

[Lub wariantowo w przypadku gdy umowę podpisują nie osoby ujawnione w KRS, a pełnomocnik:]

_____ – Pełnomocnik, na podstawie załączonego do umowy pełnomocnictwa,

zwaną dalej „**Wykonawcą**”.

[Lub wariantowo w przypadku zawarcia umowy z osobą fizyczną prowadzącą działalność gospodarczą:]

_____ prowadzącą/cym działalność gospodarczą pod firmą: _____ ze stałym miejscem wykonywania działalności w _____, ul. _____, _____, NIP _____, REGON _____, działając-ą/ym osobiście / któr-ą/ego reprezentuje _____ jako pełnomocnik na podstawie załączonego do umowy pełnomocnictwa,

zwan-ą/ym dalej „**Wykonawcą**”.

[w przypadku, gdy po stronie Zleceniobiorcy występuje konsorcjum podmiotów, należy przypisać każdemu z nich odpowiednie dodatkowe określenie: „Lider konsorcjum” / „Członek konsorcjum”]

Zamawiający i Wykonawca są również w dalszej części umowy zwani łącznie „**Stronami**”, a każdy z osobna „**Stroną**”.

Niniejsza umowa jest w dalszej jej części zwana „**Umową**”.

§ 1. PRZEDMIOT UMOWY

1. Zamawiający zamawia, a Wykonawca zobowiązuje się:

- 1) sprzedać i dostarczyć fabrycznie nowe urządzenia wielofunkcyjne (**Sprzęt, Urządzenia**), wraz z odpowiednim oprogramowaniem niezbędnym do właściwego korzystania ze Sprzętu (**Oprogramowanie**) i odpowiednimi licencjami uprawniającymi do korzystania z tego Oprogramowania (**Licencje**) oraz wsparciem producenta Oprogramowania, na podstawie zamówień składanych w miarę zaistnienia potrzeby Zamawiającego i na zasadach określonych w Umowie (**Zamówienia**). W ramach Umowy Wykonawca zobowiązuje się do wykonania także innych obowiązków określonych w Umowie, w szczególności zobowiązuje się do prawidłowego podłączenia i konfiguracji Sprzętu do funkcjonującego u Zamawiającego systemu teleinformatycznego,

- 2) sprzedać i dostarczyć oprogramowanie do zarządzania wydrukiem (**System**) wraz z odpowiednimi licencjami uprawniającymi do korzystania z tego Systemu (**Licencje**),
 - 3) wykonać wdrożenie Systemu u Zamawiającego (**Wdrożenie**),
(dalej łącznie **Przedmiot Umowy**).
2. Wykonawca zobowiązany jest do zapoznania się z „Ogólnymi Warunkami Umów Realizowanych dla Polskiej Spółki Gazownictwa sp. z o.o.” z dnia 12.05.2025 r. (**OWU**), dostępnymi na stronie internetowej Zamawiającego pod adresem www.psgaz.pl, w zakładce: **Dla kontrahenta / Pliki do pobrania**. Wykonawca oświadcza, że zapoznał się z OWU przed zawarciem Umowy, nie wnosi do nich zastrzeżeń oraz akceptuje je w całości. Strony potwierdzają, iż OWU stanowią integralną część Umowy. W przypadku rozbieżności pomiędzy postanowieniami Umowy a OWU lub innych załączników, pierwszeństwo mają postanowienia Umowy.
 3. Szczegółowy opis Przedmiotu Umowy zawiera **Załącznik Nr 1 do Umowy**. Szczegółowy opis Sprzętu i ceny jednostkowe Sprzętu zawiera **Załącznik Nr 5 do Umowy**.
 4. Zamawiający zobowiązuje się zamówić Sprzęt w wymiarze nie mniejszym niż za 80% kwoty określonej § 7 ust.1.1).
 5. Poza wymiarem określonym w ust. 4 Umowa nie zobowiązuje Zamawiającego do zamówienia Sprzętu w ilościach, które określa **Załącznik Nr 1 do Umowy**. Zamawiający zamawia Sprzęt według własnych potrzeb, a Wykonawcy nie przysługują w stosunku do Zamawiającego żadne roszczenia z tego tytułu.
 6. Wykonawca zobowiązany jest dostarczyć Sprzęt wraz Oprogramowaniem i Licencjami oraz zainstalować Sprzęt i Oprogramowanie na własny koszt i ryzyko w miejscach określonych w **Załączniku Nr 8 do Umowy**, które to miejsca Strony ustalają jako miejsce wydania Sprzętu. Dostarczenie Sprzętu obejmuje: transport, rozładunek i wniesienie Sprzętu do pomieszczenia wskazanego przez Zamawiającego, z zastrzeżeniem § 3.11.
 7. Wykonawca zobowiązany jest do zainstalowania i zintegrowania Sprzętu wraz z Oprogramowaniem ze środowiskiem teleinformatycznym Zamawiającego (o ile taka potrzeba wystąpi) oraz skutecznego uruchomienia Sprzętu wraz z Oprogramowaniem. Wykonawca zobowiązany jest niezwłocznie pisemnie (dopuszczalna jest także forma elektroniczna) poinformować Zamawiającego, jeżeli wykonanie Umowy w powyższym zakresie wymaga przekazania przez Zamawiającego informacji, specyfikacji lub innych materiałów posiadanych przez Zamawiającego.
 8. Wykonawca wraz ze Sprzętem dostarczy pełną dokumentację standardowo dostarczaną przez producentów danego sprzętu, w tym również gwarancję producenta Sprzętu oraz dokumentację potwierdzającą uprawnienia Zamawiającego do zgodnego z prawem i nienaruszającego praw osób trzecich korzystania z Oprogramowania (Licencja). Dostarczona dokumentacja musi być sporządzona w języku polskim.
 9. Zamawiający wyraża Wykonawcy zgodę na wykonanie Umowy z pomocą osób trzecich lub powierzenie wykonania Umowy osobom trzecim – z zastrzeżeniem postanowień OWU dot. podwykonawców oraz z zastrzeżeniem § 14 ust. 3 Umowy.
 10. W przypadku zmiany parametrów lub wycofania przez producenta z rynku Sprzętu oznaczonego w **Załączniku Nr 2 do Umowy**, Zamawiający dopuszcza do zaoferowania inny model Sprzętu lub zmianę jego parametrów pod poniższymi warunkami:
 - a) Wykonawca przedstawi do zaakceptowania Zamawiającemu Kartę produktu nowego Sprzętu zgodną ze specyfikacją Sprzętu określoną w **Załączniku nr 1 do Umowy**,
 - b) parametry nowego Sprzętu będą nie gorsze niż Sprzętu wycofanego, Wykonawca dostarczy Sprzęt do testów w celu potwierdzenia parametrów,
 - c) cena jednostkowa nowego Sprzętu nie może być wyższa niż dotychczasowa cena wykazana w **Załączniku Nr 5 do Umowy**.
 11. Zamawiający i Wykonawca obowiązani są współdziałać przy wykonaniu Umowy, w celu należytej realizacji zamówienia.

§ 2. OŚWIADCZENIA STRON

1. Wykonawca oświadcza, iż posiada niezbędne możliwości techniczne oraz wiedzę, potrzebne do prawidłowej realizacji Umowy oraz zobowiązuje się wykonać Umowę dochowując najwyższej staranności. Wykonawca jest zobowiązany przy wykonywaniu Umowy stosować się do wytycznych Zamawiającego.
2. Wykonawca zobowiązany jest do przestrzegania „Wymagań w zakresie BHP, Ppoż. i OŚ dla Wykonawców świadczących usługi na rzecz i terenie PSG sp. z o.o.” aktualizacja z dnia 09.10.2025 r. do Wydania 8 z dnia 26.06.2024 r. (**Wymagania**), dostępnych na stronie internetowej Zamawiającego pod adresem www.psgaz.pl, w zakładce: Dla kontrahenta / Pliki do pobrania. Wykonawca oświadcza, że zapoznał się z Wymaganiami przed zawarciem Umowy, nie wnosi do nich zastrzeżeń oraz akceptuje je w całości, jak również zobowiązuje się do zapoznania z Wymaganiami swoich pracowników oraz inne osoby, przy pomocy których będzie realizował Przedmiot Umowy.
3. Wykonawca zobowiązany jest do przestrzegania „Klauzuli Etycznej” z dnia 09.10.2025 r. (Klauzula), dostępnej na stronie internetowej Zamawiającego pod adresem www.psgaz.pl, w zakładce: Dla kontrahenta / Pliki do pobrania. Wykonawca oświadcza, że zapoznał się z Klauzulą przed zawarciem Umowy, nie wnosi do niej zastrzeżeń oraz akceptuje ją w całości, jak również zobowiązuje się do zapoznania z Klauzulą swoich pracowników oraz inne osoby, przy pomocy których będzie realizował Przedmiot Umowy.
4. Wykonawca zobowiązuje się realizować Przedmiot Umowy w sposób niezakłócający bieżącej realizacji zadań przez Zamawiającego.
5. Wykonawca zapewnia i gwarantuje, że Sprzęt wraz z Oprogramowaniem jest fabrycznie nowy, nieużywany, wyprodukowany nie wcześniej niż 12 miesięcy od daty dostarczenia, dopuszczony do obrotu i użytkowania na terenie Unii Europejskiej i będzie funkcjonować prawidłowo, zgodnie z jego specyfikacją i przeznaczeniem, oraz że jest wolny od wad fizycznych i prawnych.
6. Wykonawca oświadcza, że dostarczony Przedmiot umowy spełnia wszystkie wymagania stawiane przez Zamawiającego na etapie postępowania o udzielenie zamówienia.
7. Wykonawca oświadcza, że Sprzęt stanowi jego wyłączną własność i jest wolny od wad fizycznych i prawnych.
8. Zamawiający oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu art. 4 pkt 6) Ustawy z dnia 8 marca 2013 roku o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych.

[Postanowienie opcjonalne:]

9. Wykonawca oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu art. 4 pkt 6 ustawy z dnia 8 marca 2013 roku o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych.

§ 3. ZASADY REALIZACJI PRZEDMIOTU UMOWY

1. Każda dostawa Sprzętu będzie realizowana przez Wykonawcę na podstawie Zamówienia, którego wzór stanowi **Załącznik Nr 7 do Umowy**. Przez dostawę Sprzętu rozumie się nie tylko fizyczne dostarczenie Sprzętu, ale również dostawę Oprogramowania i Licencji na Sprzęt dostarczany w ramach danego Zamówienia oraz jego instalację u Zamawiającego, w tym podłączenie i konfigurację Sprzętu do funkcjonującego u Zamawiającego oprogramowania. Wykonawca zobowiązuje się również do przekazania Zamawiającemu dokumentów, na podstawie których Zamawiający jest uprawniony do korzystania z Oprogramowania, zgodnie z obowiązującymi przepisami prawa.
2. Zamówienie przekazywane jest Wykonawcy drogą elektroniczną (mailową) na adres e-mail: [***].
3. Osoby upoważnione przez Zamawiającego do składania Zamówień określa **Załącznik nr 9 do Umowy**. Zmiana osób upoważnionych do składania Zamówień nie stanowi zmiany Umowy, ale wymaga dla swej skuteczności powiadomienia drugiej Strony w formie pisemnej pod rygorem nieważności.
4. Zamówienie powinno określać co najmniej ilość i rodzaj Sprzętu oraz lokalizacje do których sprzęt ma zostać dostarczony, zgodnie ze Wzorem zamówienia stanowiącym **Załącznik Nr 6 do Umowy**.

5. Wykonawca będzie zobowiązany do potwierdzenia otrzymanego Zamówienia w takiej samej formie, w jakiej Zamawiający je złożył, w terminie **3 dnia roboczego** (przez co rozumie się dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w Polsce – dalej: **Dni robocze**). W przypadku braku jakiegokolwiek oświadczenia Wykonawcy w tym terminie, Zamówienie uznaje się za przyjęte do realizacji. Potwierdzenie przyjęcia Zamówienia przez Wykonawcę oznacza przyjęcie go do realizacji na warunkach określonych w Zamówieniu.
6. Jednorazowa dostawa Sprzętu, w tym czynności określonych w ust. 1 powyżej, realizowana na podstawie Zamówienia określana jest mianem „**Partii**”.
7. Wykonawca zobowiązany jest do dostawy Sprzętu w terminie wskazanym w Zamówieniu, tj. w terminie nie dłuższym niż 30 dni kalendarzowych od dnia złożenia Zamówienia. W uzasadnionych przypadkach Koordynatorzy są uprawnieni do przedłużenia terminu dostawy sprzętu wskazanego w Zamówieniu o nie więcej niż 30 dni. Odbiór Sprzętu zostanie potwierdzony pisemnym protokołem odbioru, zgodnie z wzorem stanowiącym **Załącznik Nr 6 do Umowy**.
8. Dostawy Sprzętu odbywać się będą w Dni robocze w godzinach 8:00-15:00 na adres lokalizacji i do pomieszczenia wskazanego przez Zamawiającego w Zamówieniu.
9. Odbiór Sprzętu nastąpi w lokalizacjach określonych w **Załączniku Nr 8 do Umowy**.
10. Wydanie Sprzętu odbywać się będzie z udziałem przedstawicieli Zamawiającego oraz Wykonawcy, tj. osób wskazanych w **Załączniku Nr 9 do Umowy**.
11. Zamawiający zastrzega sobie możliwość wskazania dodatkowej lokalizacji, ponad lokalizacje wskazane w **Załączniku nr 8**, do której Wykonawca dostarczy Sprzęt, a Zamawiający go odbierze. Osoba, o której mowa w ust. 3, przekaże w formie wiadomości e-mail wraz ze złożeniem Zamówienia, informację o wprowadzonej dodatkowej lokalizacji do danego Zamówienia, na adres e-mail wskazany w ust. 2. Wskazanie dodatkowej lokalizacji nie stanowi zmiany Umowy.
12. Wykonawca zobowiązuje się, że powierzy realizację Przedmiotu Umowy osobom, które zostały wskazane przez Wykonawcę na potwierdzenie warunku udziału w postępowaniu, określonego w dokumentacji postępowania o udzielenie zamówienia, w wyniku którego zawarto Umowę. Wykaz osób wraz z wymaganiami w zakresie posiadanego przez te osoby doświadczenia i kwalifikacji, określa **Załącznik nr 7 do Umowy**.
13. Powierzenie realizacji Przedmiotu Umowy osobom innym niż wskazane w wykazie osób - **Załączniku nr 7 do Umowy** - wymaga uprzedniej pisemnej zgody Zamawiającego (dopuszczalne jest także wyrażenie zgody drogą mailową) i możliwe jest tylko i wyłącznie pod warunkiem, iż nowo wskazane osoby będą spełniać wymagania określone w **Załączniku nr 7 do Umowy**. Powyżej opisana zmiana **Załącznika nr 7 do Umowy** nie stanowi zmiany Umowy.

§ 4. OKRES OBOWIĄZYWANIA UMOWY

1. Wykonawca zobowiązuje się realizować Przedmiot Umowy w zakresie sprzedaży i dostarczania Sprzętu przez okres **24 miesięcy** liczony od dnia zawarcia Umowy.
2. Jeżeli Zamówienie zostanie złożone przed upływem terminu, o którym mowa w ust. 1, a termin realizacji Zamówienia wypada po terminie o którym mowa w ust. 1, to Zamówienia podlega realizacji na warunkach określonych w Umowie.
3. Wykonawca zobowiązuje się sprzedać i dostarczyć System wraz z Licencjami oraz wykonać Wdrożenie w terminie 9 miesięcy liczonych od dnia zawarcia Umowy.
4. Warsztaty zostaną przeprowadzone w terminie 7 Dni roboczych od dnia dostarczenia pierwszej Partii. Miejsce i dokładny termin Warsztatów zostaną uzgodnione przez Koordynatorów Umowy. W razie braku uzgodnienia, miejsce i termin Warsztatów wyznacza Koordynator Zamawiającego
5. Umowa uznana zostanie za wykonaną w zakresie sprzedaży i dostarczenia Sprzętu z chwilą osiągnięcia maksymalnej kwoty wynagrodzenia, o której mowa w § 7.1.1, o ile maksymalna kwota wynagrodzenia zostanie osiągnięta przed upływem terminu realizacji Umowy określonym w ust. 1.

§ 5. WARUNKI DOSTAW SPRZĘTU

1. Wykonawca zobowiązany jest do dostarczenia na własny koszt i ryzyko do miejsc określonych w **Załączniku Nr 8**, które to miejsca Strony ustalają jako miejsce wydania Sprzętu, z

zastrzeżeniem § 3.11. Dostarczenie Sprzętu obejmuje: transport, rozładunek i wniesienie Sprzętu do pomieszczenia wskazanego przez Zamawiającego.

2. Wykonawca zobowiązany jest do zabezpieczenia przedmiotu Zamówienia przed uszkodzeniem lub zniszczeniem podczas transportu i rozładunku. W szczególności Wykonawca dostarczy przedmiot Zamówienia opakowany w sposób zabezpieczający go przed uszkodzeniem lub zniszczeniem podczas transportu lub rozładunku.
3. Dostawa Sprzętu musi być jednoznacznie oznakowana tak aby zapewnić jej identyfikację i prawidłową weryfikację. Jeżeli dostawa dotyczy więcej niż jednego rodzaju asortymentu, każdy z nich powinien być dostarczony w taki sposób, aby możliwe było ich sprawne odróżnienie i przeliczenie.
4. W przypadku, gdy termin dostawy jest dłuższy niż 30 dni kalendarzowych, Wykonawca jest zobowiązany na co najmniej 3 Dni robocze przed planowanym terminem dostarczenia powiadomić o tym Zamawiającego w formie elektronicznej (**Awizacja Dostawy**).
5. Awizując Dostawę Wykonawca powinien wskazać następujące dane:
 - 1) dane Wykonawcy;
 - 2) numer Zamówienia;
 - 3) termin dostawy;
 - 4) przedmiot dostawy.
6. Zamawiającemu przysługuje prawo do odmowy przyjęcia dostawy, gdy Wykonawca nie dokonał Awizowania Dostawy. W takim przypadku Wykonawca zobowiązany jest ponownie dostarczyć przedmiot Zamówienia w uzgodnionym z Zamawiającym terminie.

§ 6. PROCEDURA ODBIORU

1. Odbiór Przedmiotu Umowy rozumianego w niniejszy paragrafie jako odrębny odbiór: Partii, Systemu wraz z Licencjami oraz Wdrożenia zostanie potwierdzony pisemnym protokołem odbioru, podpisanym przez obie Strony bez zastrzeżeń, którego wzór stanowi **Załącznik Nr 6 do Umowy**. Zamawiający jest zobowiązany, w terminie do 7 Dni roboczych od daty zgłoszenia przez Wykonawcę gotowości do odbioru Przedmiotu Umowy, drogą mailową na adres wskazany w § 14.1.1, do jego odbioru poprzez podpisanie protokołu odbioru albo do zgłoszenia w protokole odbioru uwag co do prawidłowości realizacji Umowy przez Wykonawcę.
2. Własność, a także ryzyko utraty i uszkodzenia Sprzętu przechodzi na Zamawiającego z chwilą wykonania Przedmiotu Umowy określoną zgodnie z ust. 5 poniżej.
3. Zamawiający uprawniony jest do zgłoszenia uwag drogą mailową co do prawidłowości realizacji Przedmiotu Umowy w terminie 7 Dni roboczych od dnia zgłoszenia przez Wykonawcę gotowości do odbioru Przedmiotu Umowy. W razie zgłoszenia takich uwag Wykonawca zobowiązany jest do ich uwzględnienia w terminie 7 Dni roboczych od dnia ich zgłoszenia lub innym uzgodnionym przez Strony.
4. Po usunięciu przez Wykonawcę wszystkich wad i nieprawidłowości, o których mowa w ust. 3, Strony podpiszą protokół odbioru potwierdzający, że wszystkie wady i nieprawidłowości zostały w całości usunięte.
5. Za dzień wykonania Przedmiotu Umowy uznaje się:
 - 1) dzień podpisania przez Strony protokołu odbioru bez zastrzeżeń, o którym mowa w ust. 1 – w przypadku, gdy Zamawiający nie zgłosi uwag co do prawidłowości realizacji Przedmiotu Umowy,
 - 2) dzień podpisania przez Strony protokołu odbioru bez zastrzeżeń, o którym mowa w ust. 4 – w przypadku wniesienia przez Zamawiającego uwag co do prawidłowości realizacji Przedmiotu Umowy.
6. Przed podpisaniem protokołu odbioru Partii Wykonawca zobowiązany jest przekazać Zamawiającemu wszelkie atesty, certyfikaty i inne dokumenty potwierdzające spełnianie obowiązujących norm i dopuszczające Sprzęt do obrotu, sporządzone w języku polskim.
7. W przypadku, gdy Wykonawca nie uwzględni uwag Zamawiającego dotyczących prawidłowości realizacji Przedmiotu Umowy w terminie określonym w ust. 3, Zamawiający uprawniony jest do

odmowy przyjęcia Przedmiotu Umowy, która zostanie zwrócona w całości lub części niezgodnej z Umową albo Zamówieniem do Wykonawcy na jego koszt i ryzyko wraz z protokołem odbioru, na którym wskazano uwagi Zamawiającego.

8. Nieusunięcie wad w terminie zdefiniowanym w ust. 3 będzie traktowane jako nienależyte wykonanie Umowy i może być dla Zamawiającego powodem do odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy na zasadach i w terminie określonym w Umowie.

§ 7. WYNAGRODZENIE I ZASADY ROZLICZEŃ

1. Wykonawca za realizację Przedmiotu Umowy otrzyma łączne wynagrodzenie nieprzekraczające kwoty [***] zł (słownie: [***] złotych), w tym wynagrodzenie za:
 - 1) [***] zł (słownie: [***] złotych) za sprzedaż i dostarczenie Sprzętu wraz z **Oprogramowaniem** i Licencjami uprawniającymi do korzystania z tego Oprogramowania (**Licencje**) oraz wsparciem producenta Oprogramowania,
 - 2) [***] zł (słownie: [***] złotych) za System i za Licencje do Systemu,
 - 3) [***] zł (słownie: [***] złotych) za Wdrożenie.
2. Rozliczenie wynagrodzenia następować będzie po dostawie Partii i po realizacji każdego ze świadczeń o których mowa w § 1 ust. 1 pkt. 2-3. Wynagrodzenie za dokonaną dostawę Przedmiotu Umowy w zakresie danej Partii obliczane będzie każdorazowo jako iloczyn ceny jednostkowej oraz ilości dostarczonego Sprzętu wraz z Oprogramowaniem (w tym Licencjami). Ceny jednostkowe Sprzętu wraz z Oprogramowaniem (w tym Licencjami) określone są w **Załączniku Nr 5 do Umowy**.
3. Wynagrodzenie określone lub obliczone zgodnie z ust. 2 ma charakter ryczałtowy i obejmuje całość prac i wszelkich kosztów związanych z realizacją Umowy.
4. Wynagrodzenie wyrażone jest w kwocie netto i zostanie powiększone o podatek VAT zgodnie z przepisami prawa podatkowego.
5. Wynagrodzenie płatne będzie na podstawie prawidłowo wystawionej:
 - 1) Faktury ustrukturyzowanej przesłanej przy użyciu Krajowego Systemu e-Faktur (**KSeF**), w terminie 30 dni od dnia otrzymania faktury oraz po dostarczeniu, zgodnie z ust. 6, oryginału lub kopii podpisanego przez Strony protokołu odbioru Partii lub protokołu odbioru każdego ze świadczeń o którym mowa w § 1 ust. 1 pkt. 2-3,
 - 2) Faktury elektronicznej przesłanej zgodnie z ust. 11, na adres wskazany w ust. 15.2), z zastrzeżeniem ust. 16, w terminie 30 dni od dnia otrzymania faktury wraz z oryginałem lub kopią podpisanego przez Strony protokołu odbioru Partii lub protokołu odbioru każdego ze świadczeń o którym mowa w § 1 ust. 1 pkt. 2-3.

Podstawą do wystawienia faktury będzie wykonanie Przedmiotu Umowy w zakresie danej Partii lub każdego ze świadczeń o którym mowa w § 1 ust. 1 pkt. 2-3, stosownie do postanowień § 6.5. Do wystawienia faktury uprawniony jest *[postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum*. *[Postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum* wystawi fakturę w terminie 7 dni od dnia wykonania, o którym mowa w zdaniu poprzednim. Przez datę otrzymania faktury należy rozumieć dzień jej otrzymania w rozumieniu przepisów ustawy o podatku od towarów i usług.

6. Załączniki do faktury ustrukturyzowanej, przesłanej przy użyciu KSeF, należy przekazywać Zamawiającemu za pośrednictwem narzędzia dostępnego na stronie internetowej Zamawiającego pod adresem www.psgaz.pl, w zakładce: *Dla Kontrahenta / KSeF - Formularz załączników do faktur*.

W drodze wyjątku dopuszcza się przesłanie dokumentów:

- 1) drogą mailową na adres Koordynatora Zamawiającego wskazany w § 14.1.1);
 - 2) w postaci linku do własnych zasobów *[postanowienia wariantowe:] Wykonawcy [lub:] Lidera konsorcjum [lub:] Członka konsorcjum*, zamieszczonego na fakturze ustrukturyzowanej.
7. Strony postanawiają, że w przypadku wystawiania faktur w trybie offline24 oraz w trybie offline – niedostępność KSeF, *[postanowienia wariantowe:] Wykonawca [lub:] Lider Konsorcjum [lub:] Członek konsorcjum* będzie przysyłał faktury tylko i wyłącznie poprzez KSeF.

8. Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum zobowiązany jest wskazać na fakturze, jaka część wynagrodzenia za realizację Przedmiotu Umowy przysługuje mu z tytułu udzielenia Licencji.
9. Płatność wynagrodzenia nastąpi przelewem na rachunek bankowy [postanowienia wariantowe:] Wykonawcy [lub:] Lidera konsorcjum [lub:] Członka konsorcjum prowadzony przez bank [***] o numerze [***], wskazany na fakturze. Za dzień płatności Strony przyjmują dzień obciążenia rachunku bankowego Zamawiającego. Zmiana rachunku bankowego [postanowienia wariantowe:] Wykonawcy [lub:] Lidera konsorcjum [lub:] Członka konsorcjum jest skuteczna dla Zamawiającego z chwilą powiadomienia go przez [postanowienia wariantowe:] Wykonawcę [postanowienia wariantowe:] Lidera konsorcjum [lub:] Członka konsorcjum poprzez pisemne oświadczenie i nie stanowi zmiany Umowy. [postanowienia wariantowe:] Wykonawca [postanowienia wariantowe:] Lider konsorcjum [lub:] Członek konsorcjum oświadcza, że numer rachunku bankowego, który zostanie wskazany na fakturze jest numerem rachunku bankowego [postanowienia wariantowe:] Wykonawcy [lub:] Lidera konsorcjum [lub:] Członka konsorcjum, otwartym w związku z prowadzoną działalnością gospodarczą oraz znajduje się w wykazie, o którym mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.
10. Na fakturze [postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum wskaże:
- Dane nabywcy: Polska Spółka Gazownictwa sp. z o.o., ul. Wojciecha Bandrowskiego 16, 33-100 Tarnów, NIP 5252496411
- Dane Odbiorcy: Polska Spółka Gazownictwa sp. z o.o., Oddział Wsparcia w Warszawie, adres: ul. Krucza 6/14, 00-537 Warszawa,
- oraz następujące informacje: nr Umowy, Departament Teleinformatyki i Cyberbezpieczeństwa, termin płatności 30 dni.
11. Strony dopuszczają stosowanie faktur elektronicznych, które zostaną przesłane na adres wskazany w ust. 15.2), tylko w przypadku awarii KSeF (tryb awaryjny lub awaria całkowita), w przypadku podmiotów nieobjętych obowiązkiem wystawiania i udostępniania faktur przy użyciu KSeF albo do dnia poprzedzającego dzień, w którym [postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum obowiązany będzie do wystawiania i udostępniania faktur ustrukturyzowanych przy użyciu KSeF.
12. W przypadku, o którym mowa w ust. 11, faktury będą wystawiane i przesyłane zgodnie z obowiązującymi przepisami ustawy o podatku od towarów i usług, przy zagwarantowaniu ich autentyczności pochodzenia, integralności treści i czytelności, w postaci zabezpieczonego przed edycją pliku (to jest w formacie PDF). Pliki z fakturami skompresowane, zaszyfrowane lub w formacie innym niż spełniający wymogi przewidziane w zdaniu pierwszym albo pliki zamieszczone pośrednio w wiadomości będącej załącznikiem innej wiadomości, nie będą uważane za skutecznie doręczone faktury elektroniczne. W sposób wskazany w niniejszym ustępie należy przekazywać również pozostałe dokumenty księgowe, niebędące fakturą lub protokół odbioru w formie oryginału lub kopii.
13. Faktury wystawione w trakcie awarii KSeF (tryb awaryjny lub awaria całkowita) należy opatrzyć odpowiednimi kodami QR. Do przesłanej faktury należy dołączyć wszystkie załączniki wymagane Umową. W przypadku przesyłania faktur wystawionych w trybie awarii, [Postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum wskaże w temacie wiadomości e-mail informacje świadczące o załączeniu ww. faktur np.: „Awaria KSeF faktura/(-y)”, dodatkowo w treści wiadomości e-mail winien znajdować się wykaz wszystkich faktur załączonych w formie elektronicznej.
14. Faktury wystawione przez [postanowienia wariantowe:] Wykonawcę [lub:] Lidera konsorcjum [lub:] Członka konsorcjum, który nie jest obowiązany do wystawiania i udostępniania faktur przy użyciu KSeF, przesyłane są w formie elektronicznej na adres wskazany w ust. 15.2). [Postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum wskaże w temacie wiadomości e-mail informacje świadczące o załączeniu faktur elektronicznych np.: „faktura / korekta faktury”, zaś w treści wiadomości e-mail winien znajdować się wykaz wszystkich faktur załączonych w formie elektronicznej.
15. Strony zastrzegają, że faktury elektroniczne uznaje się za skutecznie wysłane i doręczone, tylko jeżeli zostały wysłane i odebrane przy użyciu niżej wskazanych adresów e-mail:

- 1) dla wysyłki przez [postanowienia wariantowe:] Wykonawcę [lub:] Lidera konsorcjum [lub:] Członka konsorcjum - e-mail: [***],
 - 2) dla przyjęcia przez Zamawiającego - e-mail: faktury.elektroniczne@psgaz.pl.
16. W przypadku, o którym mowa w ust. 11, gdy z przyczyn leżących po stronie [postanowienia wariantowe:] Wykonawcy [lub:] Lidera konsorcjum [lub:] Członka konsorcjum lub Zamawiającego nie jest możliwe wystawienie lub przesłanie faktury elektronicznej, Strona, u której przyczyny te wystąpią, niezwłocznie poinformuje drugą Stronę. W takiej sytuacji [postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum zobowiązany jest do doręczenia faktury, na adres: Polska Spółka Gazownictwa sp. z o.o., ul. Leona Kruczkowskiego 2, 00-412 Warszawa.
17. Zmiana adresu, o którym mowa w ust. 15 oraz ust. 16, jest skuteczna dla drugiej Strony z chwilą jej powiadomienia i nie stanowi zmiany Umowy.
18. W przypadku nieterminowej zapłaty [postanowienia wariantowe:] Wykonawca [lub:] Lider konsorcjum [lub:] Członek konsorcjum może naliczyć Zamawiającemu odsetki za opóźnienie w wysokości zgodnej z obowiązującymi w tym zakresie przepisami prawa.

§ 8. LICENCJE

1. Wykonawca oświadcza, że właścicielem autorskich praw majątkowych do Oprogramowania do zarządzania Sprzętem jest [***], właścicielem autorskich praw majątkowych do Systemu jest [***], a Wykonawca zobowiązuje się, że [***] i [***] wraz z odbiorem Oprogramowania oraz Systemu udzielił Zamawiającemu Licencji w ramach wynagrodzenia określonego w § 7.1 Umowy.
2. Wykonawca zobowiązuje się do dostarczenia Zamawiającemu dokumentów, na podstawie których Zamawiający jest uprawniony do korzystania z Oprogramowania i Systemu, zgodnie z obowiązującymi przepisami prawa, które będą stanowiły załącznik do Umowy. Dokumenty powinny wskazywać na zakres i pola eksploatacji, na których udzielana jest Licencja.
3. Udzielenie Licencji następuje z dniem, o którym mowa w § 6.5.
4. Licencja ma charakter niewyłączny i jest udzielona na czas nieokreślony na standardowych warunkach producenta Oprogramowania i producenta Systemu w zakresie wskazanym w **Załączniku Nr 1 do Umowy**.
5. Intencją Stron jest zbliżenie upoważnienia na korzystanie z Oprogramowania i z Systemu do umowy o charakterze jednorazowej transakcji podobnej do sprzedaży – w związku z tym w zamian za uiszczoną opłatę licencyjną (stanowiącą w przypadku Umowy element wynagrodzenia), Zamawiający otrzymuje ciągle, stałe i niewypowiadalne prawo do korzystania z Oprogramowania i z Systemu.
6. W przypadku gdyby postanowienie o nie wypowiedzalności licencji na Oprogramowanie i System okazało się nieskuteczne lub nieważne, a Wykonawca byłby uprawniony do wypowiedzenia licencji, Strony uzgadniają dla uprawnionego z tytułu autorskich praw majątkowych okres wypowiedzenia licencji wynoszący 10 lat ze skutkiem na koniec roku kalendarzowego, z zastrzeżeniem ustępu następnego.
7. Wykonawca zobowiązuje się nie korzystać z uprawnienia do wypowiedzenia licencji z wyjątkiem przypadków, w których Zamawiający przekroczy warunki udzielonej licencji i naruszy autorskie prawa majątkowe przysługujące Wykonawcy oraz nie zaniecha naruszenia mimo wezwania Wykonawcy skierowanego do Zamawiającego i wyznaczenia mu w tym celu na piśmie odpowiedniego terminu, nie krótszego niż 60 dni. Wezwanie musi być wystosowane w formie pisemnej pod rygorem braku skutków i musi zawierać wyraźne zastrzeżenie, że Wykonawca będzie uprawniony do wypowiedzenia licencji w przypadku niezaprzestania dopuszczania się przez Zamawiającego wyraźnie i precyzyjnie wymienionych naruszeń. W przypadku wypowiedzenia licencji z tej przyczyny termin wypowiedzenia Licencji wynosi jeden rok, ze skutkiem na koniec roku kalendarzowego. Wykonawca oświadcza i gwarantuje, że producent programu komputerowego, gdyby nie był nim Wykonawca, będzie przestrzegał powyższych zobowiązań.
8. Licencja uprawnia Zamawiającego do korzystania z Oprogramowania na Sprzęcie i z Systemu
...

9. Przeniesienie na Zamawiającego prawa własności nośników, na których utrwalono Oprogramowanie, następuje z chwilą wydania takich nośników Zamawiającemu.
10. Jeżeli w okresie trwania Licencji Zamawiający utraci uprawnienie do korzystania z Oprogramowania lub Systemu lub ich części, bez względu na przyczynę utraty takiego uprawnienia, Wykonawca niezwłocznie, nie później niż w terminie 7 Dni roboczych od daty otrzymania zgłoszenia od Zamawiającego, na swój koszt i według swego wyboru wykona którąkolwiek z poniższych czynności naprawczych:
 - 1) udzieli ponownie/zapewni ponowne udzielenie nieodpłatnej licencji na takie Oprogramowanie, System lub ich część,
 - 2) uzyska dla Zamawiającego nieodpłatne prawo do kontynuowania używania Oprogramowania lub Systemu,
 - 3) dokona na swój koszt wymiany Oprogramowania na nienaruszające praw autorskich lub innych praw osób trzecich, a posiadające te same parametry i spełniające te same funkcje co Oprogramowanie lub System, lub
 - 4) zapewni inne rozwiązanie funkcjonalne, pozwalające Zamawiającemu na nieprzerwane korzystanie z Przedmiotu Umowy w tym samym zakresie.
11. Wykonawca zobowiązuje się podjąć wszelkie niezbędne działania w celu zabezpieczenia Zamawiającego przed jakimikolwiek działaniami osób trzecich zmierzającymi do dochodzenia ich praw w zakresie własności intelektualnej Oprogramowania lub Systemu. W przypadku, gdy osoba trzecia zwróci się do Zamawiającego z roszczeniami związanymi z Przedmiotem Umowy lub jego poszczególnymi elementami, Wykonawca zwolni Zamawiającego z obowiązku zaspokojenia takich roszczeń oraz pokryje wszelkie uzasadnione, niezbędne koszty, wydatki, opłaty, wynagrodzenia poniesione przez Zamawiającego w związku z tymi roszczeniami, jak również pokryje szkodę poniesioną przez Zamawiającego. W takim przypadku Wykonawca ponosi odpowiedzialność względem Zamawiającego za to, że osoby trzecie nie będą dochodziły zaspokojenia swoich roszczeń bezpośrednio od Zamawiającego.

§ 9. KARY UMOWNE

1. Zamawiający jest uprawniony do obciążenia Wykonawcy następującymi karami umownymi:
 - 1) za niewykonanie Przedmiotu Umowy w zakresie danej Partii w terminie wskazanym w Umowie, chyba że Wykonawca nie ponosi winy za niewykonanie w terminie Przedmiotu Umowy w zakresie danej Partii – w wysokości 0,15 % wynagrodzenia netto należnego za daną Partię, której niewykonania kara umowna dotyczy, za każdy rozpoczęty dzień opóźnienia,
 - 2) za niewykonanie Przedmiotu Umowy w zakresie któregośkolwiek ze świadczeń o którym mowa w § 1 ust. 1 pkt 2-3 w terminie wskazanym w Umowie, chyba że Wykonawca nie ponosi winy za niewykonanie w terminie Przedmiotu Umowy w zakresie któregośkolwiek ze świadczeń o którym mowa w § 1 ust. 1 pkt 2-3 – w wysokości 0,15 % wynagrodzenia netto należnego za dane świadczenie, którego niewykonania kara umowna dotyczy, za każdy rozpoczęty dzień opóźnienia,
 - 3) za uchybienie z winy Wykonawcy terminowi potwierdzenia zgłoszenia o którym mowa w § 11 ust. 17 pkt. 2 – w wysokości 200,00 PLN, za każdy przypadek nie potwierdzenia zgłoszenia.
 - 4) za nieterminowe usunięcie wad Sprzętu w okresie gwarancji, chyba że Wykonawca nie ponosi winy za niewykonanie tego obowiązku w terminie – w wysokości 0,15 % wynagrodzenia netto należnego za daną Partię, w ramach której wadliwy Sprzęt został dostarczony, za każdy rozpoczęty dzień opóźnienia,
 - 5) za nieterminowe usunięcie Wad, Awarii lub Usterek Systemu w okresie wsparcia powdrożeniowego, chyba że Wykonawca nie ponosi winy za niewykonanie tego obowiązku w terminie – w wysokości 0,15 % wynagrodzenia netto należnego za System i za Licencje do Systemu, odpowiednio za każdą rozpoczętą godzinę lub każdy rozpoczęty Dzień roboczy opóźnienia,
 - 6) za naruszenie postanowień § 7 OWU dotyczących bezpieczeństwa i ochrony informacji – w wysokości 10 % wynagrodzenia netto określonego w § 7.1, za każde naruszenie,

- 7) w razie wypowiedzenia lub odstąpienia od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy (niezależnie od podstawy prawnej) – w wysokości 10 % wynagrodzenia netto określonego w § 7.1,
 - 8) w przypadku powierzenia realizacji Przedmiotu Umowy w zakresie funkcji wskazanych w **Załączniku nr 10** do Umowy osobie, która nie jest w nim wymieniona - w wysokości 200,00 PLN za każde naruszenie.
2. Łączna wysokość kar umownych przysługujących Zamawiającemu na podstawie Umowy nie może przekroczyć 20% wynagrodzenia netto określonego w § 7.1. W celu uniknięcia wątpliwości, Strony potwierdzają, że stosownie do § 4 ust. 2 OWU, Zamawiający jest uprawniony do dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.

§ 10. ZAKOŃCZENIE UMOWY

1. Każda ze Stron ma prawo odstąpić od Umowy na zasadach określonych w § 5 OWU. Uprawnienie do odstąpienia od Umowy może zostać zrealizowane w terminie 60 Dni roboczych od dnia zaistnienia przesłanek uzasadniających odstąpienie od Umowy, jednak nie później niż do dnia upływu okresu jej realizacji określonego w § 4 Umowy.
2. Zamawiającemu przysługuje prawo do odstąpienia od Umowy w całości lub w części w przypadku:
 - 1) gdy Wykonawca utraci uprawnienie do korzystania z Oprogramowania lub jego części, bez względu na przyczynę takiej utraty, na które to Oprogramowanie uzyskał Licencję stosownie do postanowień Umowy, a Wykonawca nie wykona swojego zobowiązania, o którym mowa w § 8.10 w terminie tam wskazanym,
 - 2) jeżeli producent Oprogramowania wypowie którąkolwiek Licencję (umowę licencyjną) lub odstąpi od takiej Licencji (umowy licencyjnej) - niezależnie od tego, czy Wykonawca wykona swoje zobowiązanie, o którym mowa w § 8.10.
3. W przypadku rozwiązania Umowy, niezależnie od przyczyny, Wykonawca jest uprawniony do żądania wynagrodzenia należnego wyłącznie z tytułu należycie wykonanej części Umowy.

§ 11. GWARANCJA JAKOŚCI

1. W ramach realizacji Przedmiotu Umowy Wykonawca udziela gwarancji na Sprzęt (przez co rozumiane jest także udzielenie gwarancji na Oprogramowanie), niezależnie od gwarancji producenta Sprzętu, na okres 60 miesięcy lub zgodnie z gwarancją producenta, w zależności, która jest dłuższa. Okres gwarancji liczony jest od dnia wykonania Przedmiotu Umowy. Gwarancja dla Sprzętu wygasa w przypadku, gdy Sprzęt osiąga limit wydruków cyklu życia Urzędnika.
2. Gwarancja obejmuje wady fizyczne, wady materiałowe, wady jakościowe i wady w funkcjonalności Sprzętu.
3. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do przyjmowania zgłoszeń o wadach Sprzętu, diagnostyki wad Sprzętu, niezwłocznej naprawy lub wymiany wadliwego Sprzętu na nowy, wolny od wad.
4. Całkowity czas naprawy Sprzętu nie może przekroczyć 7 Dni roboczych, natomiast wymiany Sprzętu na nowy nie może przekroczyć 14 Dni roboczych, liczonych od dnia zgłoszenia wady. Jeżeli Wykonawca nie naprawi Sprzętu w terminie 7 Dni roboczych, uznaje się automatycznie, że podjął decyzję o wymianie Sprzętu na nowy, wolny od wad. W takiej sytuacji Zamawiający może już według swojego wyboru żądać dalszej naprawy albo wymiany.
5. Termin wykonania wymiany lub naprawy Sprzętu liczony jest od momentu zgłoszenia wady przez Zamawiającego do momentu dostarczenia do Zamawiającego nowego niewadliwego lub naprawionego Sprzętu. Przedłużenie czasu naprawy lub wymiany może nastąpić jedynie za zgodą Zamawiającego wyrażoną na piśmie i być usprawiedliwione nadzwyczajnymi trudnościami wykonania naprawy lub wymiany w terminie określonym w ust. 4 powyżej.
6. Serwis gwarancyjny będzie świadczony w miejscu wskazanym przez Zamawiającego, przy czym jeśli naprawa odbywa się u Zamawiającego, może odbywać się w jego godzinach pracy, jeżeli nie powoduje to utrudnień w bieżącej realizacji zadań przez Zamawiającego.

7. Każdy dostarczony Sprzęt winien posiadać informacje o konfiguracji wraz z informacją o poziomie gwarancji oraz o terminie jej rozpoczęcia i zakończenia z możliwością sprawdzenia tych informacji na stronie producenta Sprzętu.
8. Zamawiający zastrzega sobie prawo zachowania dysków twardych z danymi wchodzących w skład Sprzętu w przypadku potrzeby wysłania sprzętu do firmy serwisującej.
9. Za moment dostarczenia nowego lub naprawionego Sprzętu uznaje się dzień podpisania protokołu jego odbioru przy odpowiednim zastosowaniu przepisów dotyczących odbioru Przedmiotu Umowy.
10. W przypadku 3-krotnej nieskutecznej naprawy tego samego elementu w okresie gwarancji Wykonawca zobowiązany jest wymienić Sprzęt na nowy..
11. W przypadku niedokonania wymiany lub naprawy Sprzętu w terminie, o którym mowa w ust. 4, z zastrzeżeniem ust. 5, Zamawiający ma prawo zlecić naprawę Sprzętu osobom trzecim na koszt i ryzyko Wykonawcy, informując Wykonawcę o podjętym działaniu. Strony uznają to uprawnienie za uzgodnione na zasadzie swobody umów wynikającej z art. 3531 Kodeksu cywilnego.
12. Okres trwania gwarancji ulega przedłużeniu o czas, jaki był potrzebny na usunięcie wad Sprzętu.
13. Naprawa lub wymiana Sprzętu zostanie zapisana w dokumentacji gwarancyjnej Sprzętu.
14. W przypadku wymiany Sprzętu na nowy wolny od wad, gwarancja na ten Sprzęt liczona jest od momentu dostarczenia Sprzętu nowego wolnego od wad.
15. Wykonawca gwarantuje, że dostarczony Sprzęt jest fabrycznie nowy, nieużywany, wyprodukowany nie wcześniej niż 6 miesięcy od daty złożenia Zamówienia, dostarczany oficjalnym kanałem dystrybucyjnym producenta Sprzętu, wolny od wad fizycznych i prawnych.
16. Do zakupionego Sprzętu Zamawiający oczekuje zagwarantowania przez Wykonawcę serwisu gwarancyjnego określonego jak niżej:
 - 1) zgłoszenia w ramach Help Desk będą przyjmowane telefonicznie i poprzez wiadomości e-mail, w ramach systemu HelpDesk Wykonawcy udostępnionego Zamawiającemu w godzinach 8.00 – 16.00 w dni robocze (rozumiane jako dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy),
 - 2) Wykonawca niezwłocznie, nie później jednak niż w terminie 1 Dnia roboczego, potwierdza Zamawiającemu na adres e-mail: [***], otrzymanie zgłoszenia dokonanego na zasadach określonych w pkt. 1) powyżej,
 - 3) Niezależnie od postanowień pkt 2 powyżej, czas reakcji serwisu gwarancyjnego w celu podjęcia działań zmierzających do usunięcia wad musi nastąpić do końca następnego Dnia roboczego po otrzymanym zgłoszeniu o którym mowa w pkt. 1),
 - 4) czas reakcji serwisu gwarancyjnego – do końca następnego dnia roboczego po otrzymanym zgłoszeniu. Serwis gwarancyjny świadczony musi być w lokalizacji Zamawiającego w następnym dniu roboczym: wysłanie technika serwisowego do lokalizacji Zamawiającego w celu usunięcia usterki, w tym wymiany uszkodzonego elementu na miejscu w przypadku braku możliwości naprawy, Obsługa serwisu gwarancyjnego, wymiana uszkodzonych elementów, wraz z dojazdem serwisanta jest bezpłatna.
 - 5) w przypadku, kiedy nie jest możliwe wykonanie naprawy na miejscu, Wykonawca na czas naprawy wymieni naprawiany Sprzęt na zastępczy Sprzęt o parametrach nie gorszych od Sprzętu naprawianego oraz poprowadzi współpracę z oprogramowaniem SafeCom i nie później niż do końca 2 kolejnych dni roboczych. Sprzęt zastępczy zostanie dostarczony i odebrany przez Wykonawcę i na koszt Wykonawcy,
 - 6) Zamawiający zastrzega sobie prawo zachowania dysku twardego z danymi, wchodzącego w skład Sprzętu w przypadku potrzeby wysłania Sprzętu do firmy serwisującej,
 - 7) serwis gwarancyjny będzie realizowany przez autoryzowanego przedstawiciela producenta – firma serwisująca musi posiadać certyfikat ISO 9001 lub równoważny, na świadczenie usług serwisowych oraz posiadać autoryzację producenta sprzętu, a w przypadku nie wywiązywania się z obowiązków gwarancyjnych przez wykonawcę, producent oferowanych urządzeń, przejmie zobowiązania związane z serwisem gwarancyjnym urządzeń. Przez certyfikat równoważny należy rozumieć obowiązujący certyfikat, co najmniej: wystawiony przez akredytowaną jednostkę uprawnioną do poświadczania spełnienia przez Wykonawcę

określonych norm zapewnienia jakości oraz obejmujący tożsamy zakres z żądanym certyfikatem,

- 8) w ramach gwarancji przez okres jej obowiązywania, o którym mowa w pkt. 4.1, Wykonawca zapewni dla każdego zakupionego Urządzenia wielofunkcyjnego 10 bezpłatnych przeglądów konserwacyjnych (2 w każdym roku w odstępie co najmniej 5 miesięcy),
- 9) zakres przeglądów konserwacyjnych powinien obejmować wykonanie następujących czynności:
 - a) wykonanie kopii testowych oraz sprawdzenie liczników zacięć i kodów serwisowych,
 - b) smarowanie elementów napędów jeśli jest to wymagane przez producenta,
 - c) czyszczenie modułów (zespołu optyki, zespół tworzenia, wywoływania i przenoszenia obrazu, zespół podawania, transportu papieru, zespół podawania, transportu dokumentów, zespół utrwalania obrazu),
 - d) czyszczenie obudowy,
 - e) kalibracja kolorów,
 - f) wykonanie kopii testowej,
 - g) aktualizacja oprogramowania Urządzenia na życzenie Zamawiającego,
 - h) wymianę materiałów eksploatacyjnych dostarczonych przez Zamawiającego, dla których producent określił wymóg wymiany tylko przez autoryzowany serwis,
 - i) przygotowanie raportu z informacją o konieczności wymiany niezbędnych materiałów eksploatacyjnych.
17. Koszty i ryzyka wszelkich świadczeń gwarancyjnych, w tym przeglądów konserwacyjnych ponosi Wykonawca i są one ujęte w cenie sprzedaży Sprzętu.
18. Warunki wsparcia powdrożeniowego Systemu zawiera pkt 13 Załącznika nr 2.

§ 12. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

1. Wykonawca zobowiązany jest do wniesienia zabezpieczenia należytego wykonania Przedmiotu Umowy zgodnie z zasadami określonymi w § 10 OWU.
2. Strony oświadczają, że Wykonawca wniósł zabezpieczenie należytego wykonania Przedmiotu Umowy przed zawarciem Umowy.
3. Wysokość zabezpieczenia należytego wykonania Przedmiotu Umowy stanowi 3% wartości wynagrodzenia, o którym mowa w § 7.1 powiększonego o podatek VAT, tj. kwotę [***] zł (słownie: [***]).
4. Wykonawca może wnieść zabezpieczenie w jednej lub kilku formach, o których mowa w § 10.4 OWU.
5. Zamawiający ma prawo do pozostawienia kwoty [***] zł (słownie: [***] złotych) [kwota stanowiąca 30 % wysokości zabezpieczenia] na zabezpieczenie roszczeń z tytułu rękojmi za wady lub gwarancji jakości Przedmiotu Umowy.

§ 13. UBEZPIECZENIA

Wykonawca zobowiązany jest do posiadania ogólnego ubezpieczenia odpowiedzialności cywilnej przez cały okres realizacji Umowy, zgodnie z zasadami określonymi w § 11 OWU.

§ 14. OSOBY ODPOWIEDZIALNE ZA REALIZACJĘ UMOWY I DORECZENIA

1. Każda ze Stron powołuje swojego przedstawiciela do bieżących kontaktów, który będzie nadzorować sprawną realizację Umowy, zwanego dalej Koordynatorem:
 - 1) Koordynatorami ze strony Zamawiającego są:
[***], tel. [***], e-mail: [***];
[***], tel. [***], e-mail: [***].

- 2) Koordynatorem ze strony Wykonawcy jest: [***], tel. [***], e-mail: [***].
2. Koordynatorzy są umocowani do dokonywania w szczególności następujących czynności:
 - 1) dokonywania i przesyłania do Wykonawcy Zamówień,
 - 2) Koordynator Zamawiającego do dokonywania zgłoszeń w zakresie wskazywania dodatkowej lokalizacji,
 - 3) Koordynator Wykonawcy do akceptacji lub odmowy przyjęcia zgłoszenia w zakresie wskazania dodatkowej lokalizacji,
 - 4) akceptacji protokołu/protokołów odbioru potwierdzającego/potwierdzających wykonanie Przedmiotu Umowy,
 - 5) wyrażenia zgody na zmianę osób pełniących dane funkcje, wskazanych w **Załączniku nr 10 do Umowy**, zgodnie ust. 3,
 - 6) powiadamiania drugiej Strony o zmianie osoby Koordynatora oraz adresu do doręczeń,
 - 7) innych czynności, które wykonują Koordynatorzy, wymienionych w Umowie.
3. Strony ustalają następujące adresy do doręczeń:
 - 1) dla Zamawiającego – adres: Polska Spółka Gazownictwa sp. z o.o. Oddział Wsparcia w Warszawie, ul. Krucza 6/14, 00-537 Warszawa,
 - 2) dla Wykonawcy – adres: [***].
4. Zmiana osoby Koordynatora jest skuteczna dla drugiej Strony z chwilą jej powiadomienia. W przypadku zmiany adresu, o którym mowa w ust. 5, Strony zobowiązują się do niezwłocznego pisemnego powiadomienia drugiej Strony o nowym adresie do doręczeń, pod rygorem uznania za skutecznie doręczoną korespondencję wysłaną na dotychczasowy adres. Zmiana osoby Koordynatora lub adresu do doręczeń nie stanowi zmiany Umowy.
5. W przypadku gdy Strona składa oświadczenie w formie pisemnej powinno ono zostać doręczone za potwierdzeniem odbioru, osobiście lub na adres Strony wskazany w ust. 5. Za dzień doręczenia korespondencji uważa się dzień odbioru korespondencji przez adresata. W razie niemożności doręczenia pisma wysłanego przesyłką poleconą lub kurierską z przyczyn dotyczących Strony będącej adresatem, w szczególności w przypadku odmowy odbioru pisma przez Stronę lub zmiany adresu, pismo uważa się za skutecznie doręczone w dniu, w którym zostało nadane w polskiej placówce pocztowej operatora publicznego albo złożono zlecenie jego doręczenia podmiotowi wykonującemu działalność pocztową (świadczącemu usługi kurierskie).

§ 15. POSTANOWIENIA KOŃCOWE

1. Wszelkie zmiany Umowy, jak również jej rozwiązanie, wypowiedzenie i odstąpienie, wymagają formy pisemnej pod rygorem nieważności.
2. W kwestiach nieuregulowanych postanowieniami Umowy zastosowanie mają przepisy prawa powszechnie obowiązującego, w tym przepisy Kodeksu cywilnego.
3. Wszelkie spory mogące wynikać na tle wykonywania postanowień Umowy będą rozstrzygane przez sąd powszechny właściwy dla miejsca siedziby Oddziału Zamawiającego tj. Oddziału Wsparcia w Warszawie
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym egzemplarzu dla każdej ze Stron.

[Lub wariantowo jeżeli Umowa jest podpisywana elektronicznym podpisem kwalifikowanym przez każdą ze Stron:]

Umowa sporządzona została w jednym egzemplarzu, podpisanym elektronicznymi podpisami kwalifikowanymi, który został udostępniony każdej ze Stron.

§ 16. ZAŁĄCZNIKI

Integralną część Umowy stanowią następujące załączniki:

Załącznik Nr 1

Szczegółowy opis Przedmiotu Umowy

Załącznik Nr 2	Wymagania i wdrożenie oprogramowania równoważnego w zakresie SafeCom
Załącznik nr 3	Wymagania techniczne
Załącznik nr 4	Wymagania bezpieczeństwa
Załącznik Nr 5	Oferta Wykonawcy
Załącznik Nr 6	Wzór protokołu odbioru
Załącznik Nr 7	Wzór Zamówienia
Załącznik Nr 8	Wykaz lokalizacji dostaw i osób upoważnionych do odbioru dostaw
Załącznik Nr 9	Wykaz osób upoważnionych do składania Zamówień
Załącznik Nr 10	Wykaz osób przy pomocy, których będzie realizowany Przedmiot Zamówienia
Załącznik Nr 11	Karta materiałów do Urządzenia
Załącznik Nr 12	Klauzula antykorupcyjna

PODPISY:

Zamawiający:

Wykonawca:

Szczegółowy opis Przedmiotu Umowy

1. Opis stanu bieżącego

W Polskiej Spółce Gazownictwa sp. z o.o. funkcjonuje Centralny System Wydruku oparty na oprogramowaniu SafeCom, SprintCapture (SPC-FM) oraz ZPD Report.

SPCFM (SprintCapture Fleet Meter) to oprogramowanie wdrożone u Zamawiającego do zarządzania rozproszoną flotą urządzeń drukujących, obsługi umów serwisowych na Urządzenia drukujące (zgłoszenia napraw i konserwacji), monitorowania wykorzystania drukarek jak i aktualnego stanu zużycia materiałów eksploatacyjnych w poszczególnych Urządzeniach.

ZPD Report zlicza wydruki realizowane na drukarkach i Urządzeniach wielofunkcyjnych podłączonych do systemu, umożliwia weryfikację ilości wydrukowanych dokumentów zarówno przez pracowników jak i ich przełożonych

2. Opis przedmiotu zamówienia

2.1 Przedmiotem zamówienia jest dostawa Sprzętu o parametrach podanych poniżej.

2.1.1 Urządzenie wielofunkcyjne druk kolorowy A3 do zastosowań biurowych — 200 sztuk

Właściwości	Parametry minimalne
Technologia druku	druk laserowy lub LED
Szybkość druku w mono tryb draft	Minimum 45 stron formatu A4/min.
Rozdzielczość rzeczywista druku	Minimum 1200x1200 dpi
Czas wydruku pierwszej strony-kolor/mono	nie więcej niż 12 sekund
Podajniki papieru	minimum cztery podajniki na papier w tym ręczny na 100 arkuszy
Moduł druku dwustronnego	Tak
Obsługiwane formaty papieru	Minimum A3
Odbiornik papieru	Na minimum 500 arkuszy przy gramaturze 75 g/m ²
Pamięć	Minimum 4GB, szyfrowany dysk: SSD minimum 256 GB lub HDD minimum 500 GB
Używane języki druku	PCL 6, PCL5, Postscript 3, PDF lub emulacje
Obciążenie miesięczne/cyklu życia Urządzenia	nie mniej niż 18.000 stron/miesiąc / nie mniej niż 1.080.000 stron
Interfejsy	USB 2.0, 10/100/1000Base-TX
Skaner	Skaner kolorowy, płaski o rozdzielczości optycznej minimum 600x600 dpi, dwustronny jednoprzebiegowy (skanowane jednocześnie obie strony dokumentu w jednym przejściu)
Skanowanie sieciowe	E-mail (szyfrowanie TLS 1.2 lub TLS 1.3), FTP, folder sieciowy (obsługa protokołu SMB v3)
Podajnik dokumentów do skanera	automatyczny, z automatyczną obsługą dokumentów dwustronnych, na minimum 130 arkuszy

Szybkość faksu	33,6 kb/s
Panel sterowania Urządzenia	Dotykowy, min. 10", w języku polskim
Zużycie energii elektrycznej według wskaźnika TEC	Poniżej 2 kWh
Instrukcja obsługi	w języku polskim
Sterowniki	płyta CD lub inny nośnik typu pendrive ze sterownikami w języku polskim dla Windows Server 2016, 2019, 2022 oraz nowszy / Windows 10, 11
Wymagania dodatkowe	Obsługiwana gramatura nośników – 60 - 190 g/m2 Do każdego Urządzenia dostarczone zostaną dodatkowo: zestawy (C,M,Y,BK) tonerów każdy zestaw na minimum 100.000 wydruków mono oraz 60.000 wydruków kolorowych. Dostarczone tonery muszą być całkowicie nowe, nieużytkowane wcześniej i nieregenerowane, wyprodukowane przez producenta oferowanych urządzeń, nie może powodować utraty gwarancji producenta na sprzęt. Wykonawca wskaże adres strony internetowej producenta potwierdzający wydajność oferowanego tonera lub dołączy oświadczenie producenta o wydajności tonera.

2.1.2 Urządzenie wielofunkcyjne druk kolorowy A4 do zastosowań biurowych — 80 sztuk

Właściwości	Parametry minimalne
Technologia druku	druk laserowy lub LED
Szybkość druku w mono i kolorze, tryb draft	Minimum 40 stron formatu A4/min.
Rozdzielczość rzeczywista druku	Minimum 600x600 dpi
Czas wydruku pierwszej strony- kolor/mono	nie więcej niż 11 sekund
Podajniki papieru	2 podajniki o łącznej pojemności minimum 600 arkuszy w tym podajnik ręczny na 100 arkuszy
Moduł druku dwustronnego– automatyczny	tak
Obsługiwane formaty papieru	Minimum A4
Odbiornik papieru	Na minimum 200 arkuszy przy gramaturze 75 g/m2.
Pamięć	Minimum 3GB; szyfrowany dysk: SSD minimum 256 GB lub HDD minimum 500 GB
Używane języki druku	PCL 6, PCL5, Postscript 3, PDF lub emulacje
Obciążenie miesięczne/cyklu życia Urządzenia	nie mniej niż 5.000 stron/miesiąc / nie mniej niż 300 000 stron
Interfejsy	USB 2.0, 10/100/1000Base-TX
Skanner	Skanner kolorowy, płaski o rozdzielczości optycznej minimum 600x600 dpi, dwustronny jednoprzebiegowy (skanowane jednocześnie obie strony dokumentu w jednym przejściu)

Skanowanie sieciowe	E-mail (szyfrowanie TLS 1.2 lub TLS 1.3), FTP, folder sieciowy (obsługa protokołu SMB v3)
Podajnik dokumentów do skanera	automatyczny, z automatyczną obsługą dokumentów dwustronnych, na minimum 80 arkuszy
Szybkość faksu	33,6 kb/s
Panel sterowania Urządzenia	Dotykowy, min. 7", w języku polskim
Zużycie energii elektrycznej według wskaźnika TEC	Poniżej 2 kWh
Instrukcja obsługi	w języku polskim
Sterowniki	płyta CD lub inny nośnik typu pendrive ze sterownikami w języku polskim dla Windows Server 2016, 2019, 2022 oraz nowszy / Windows 10
Wymagania dodatkowe	Obsługiwana gramatura nośników – 60 - 190 g/m ² Do każdego Urządzenia dostarczone zostaną dodatkowo: zestawy (C,M,Y,BK) tonerów każdy zestaw na minimum 45.000 wydruków mono oraz 32.000 wydruków kolorowych. Dostarczone tonery muszą być całkowicie nowe, nieużytkowane wcześniej i nieregenerowane, wyprodukowane przez producenta oferowanych urządzeń, nie powodujące utraty gwarancji producenta na sprzęt. Wykonawca wskaże adres strony internetowej producenta potwierdzający wydajność oferowanego tonera lub dołączy oświadczenie producenta o wydajności tonera.

3. Pozostałe wymagania dla Urządzeń wielofunkcyjnych:

- 3.1. Urządzenia muszą posiadać możliwość skanowania i kopiowania dwustronnego oraz skanować dokumenty do plików o formatach takich jak: jpg, pdf, tiff.
- 3.2. Możliwość zarządzania Urządzeniem zdalnie za pośrednictwem zdalnego panelu Urządzenia oraz dostępnego panelu administracyjnego Urządzenia przez www. Możliwość zarządzania Urządzeniem lokalnie z poziomu menu administratora.
- 3.3. Możliwość podłączenia finisher'a dla urządzeń A3.
- 3.4. Wszystkie Urządzenia muszą zostać dostarczone jako gotowe do pracy, tj. muszą być wyposażone w pełnowartościowe materiały eksploatacyjne (niedopuszczalne jest dostarczenie Urządzeń z zainstalowanymi materiałami eksploatacyjnymi tzw. startowymi) oraz posiadać wszelkie potrzebne wyposażenie dodatkowe, konieczne do uruchomienia Urządzenia (takie jak kable zasilające).
- 3.5. Zamawiający wymaga, aby dostarczone Urządzenia były fabrycznie nowe, nierefabrykowane, nieużywane, wyprodukowane nie wcześniej niż 12 miesięcy od daty dostarczenia, wolne od wad fizycznych i prawnych. Dostarczane Urządzenia i tonery muszą pochodzić z oficjalnego kanału dystrybucji danego producenta na terenie Rzeczypospolitej Polskiej.
- 3.6. Wykonawca musi przekazać Zamawiającemu, przed dostarczeniem Urządzenia wielofunkcyjnego, instrukcję obsługi (dla użytkownika) dla każdego z typów dostarczanych Urządzeń.
- 3.7. Wykonawca na swój wyłączny koszt i ryzyko dostarczy przedmiot zamówienia do miejsc wskazanych przez Zamawiającego. Dostawa obejmuje również wniesienie Urządzeń do wskazanych miejsc przez Zamawiającego. Koszty załadunku, transportu, rozładunku oraz wniesienia Urządzeń obciążają Wykonawcę. Wszystkie odpady powstałe podczas realizacji zamówienia Wykonawca jest zobowiązany zagospodarować na własny koszt, Wykonawca po dostarczeniu przedmiotu zamówienia oraz po zakończeniu prac montażowych jest zobowiązany do uporządkowania terenu dostaw i miejsca montażu.
- 3.8. Wykonawca wraz z Urządzeniami dostarczy oprogramowanie do zarządzania nimi – w przypadku gdy PSG nie posiada takiego oprogramowania, o następującej funkcjonalności:
 - 1) monitorowania stanu Urządzenia drukującego,

- 2) możliwość cyklicznie zdefiniowanego przeszukiwania sieci LAN\WAN Zamawiającego w celu wyszukiwania nowych urządzeń,
 - 3) zdalna aktualizacja firmware (mikrokodów),
 - 4) możliwość wykonania restartu Urządzenia,
 - 5) możliwość konfiguracji ustawień (SMTP, SMB,SNMP) na Urządzeniu,
 - 6) rozwiązanie musi posiadać możliwość konfigurowalnego raportowania,
- oprogramowanie zapewni powyższe funkcjonalności dla jednego, jak i wielu urządzeń jednocześnie.

Obecnie PSG wykorzystuje następujące oprogramowanie:

- Xerox CentreWare Web
- HP Web Jet Admin
- PageScope Enterprise Suite

3.9. Wykonawca wraz z dostarczeniem oprogramowania, o którym mowa w pkt. 3.8. dostarczy kompleksowe usługi instalacji i uruchomienia zaoferowanego oprogramowania. Usługi muszą obejmować fizyczną instalację wszystkich elementów, uruchomienie poszczególnych komponentów i ich konfigurację według wytycznych Zamawiającego. Oprogramowanie zarządzające musi zostać zainstalowane na serwerze w infrastrukturze PSG dostarczoną przez Zamawiającego o parametrach uzgodnionych z Wykonawcą. Dostarczone oprogramowanie nie może wymagać przesyłania danych do serwerów zewnętrznych.

3.10. Zamawiający zapewnia infrastrukturę techniczną (w tym licencje bazodanowe) wymaganą do uruchomienia Systemu. Wykonawca przy współpracy z Zamawiającym określi wymagania dotyczące środowiska sprzętowego, tak żeby System był bezpieczny, wydajny i stabilny, przy czym na potrzeby realizacji projektu Zamawiający dostarczy środowisko w postaci maszyn wirtualnych Vmware vSphere 8 lub nowsze o sumarycznej ilości zasobów: 256GB pamięci operacyjnej (vRAM), 128 procesorów wirtualnych (vCPU) oraz 1 TB przestrzeni dyskowej (vDISK) na dyskach SSD i 2 TB przestrzeni dyskowej (vDISK) na dyskach magnetycznych.

3.11. Wykonawca dostarczy również potrzebne licencje na dostarczone oprogramowanie lub przedłuży licencje na posiadane przez PSG oprogramowanie (jeżeli takiego przedłużenia wymagają) wymienione w punkcie 3.8.. Dostarczona licencja musi być objęta minimum 5-cio letnią gwarancją producenta.

3.12. Wykonawca w ramach realizacji pierwszej Partii i w ramach określonego w Umowie wynagrodzenia, przeprowadzi instalację Sprzętu i przekaże wiedzę personelowi Zamawiającego z zakresu dostarczonego rozwiązania zarządzania Urządzeniami drukującymi. Instruktaż zostanie przeprowadzony dla 4 administratorów Zamawiającego w siedzibie Zamawiającego bądź w formie wideokonferencji w terminie 7 Dni roboczych od dnia dostarczenia pierwszej Partii Urządzeń. Miejsce i dokładny termin zostaną uzgodnione przez Koordynatorów Umowy.

3.13. Wykonawca zapewni gwarancję techniczną w zakresie dostarczonego lub posiadanego przez PSG oprogramowania zarządzającego na okres trwania gwarancji dostarczonych Urządzeń drukujących. Gwarancja musi obejmować między innymi:

- 1) W okresie gwarancji na zakupione Urządzenia drukujące, Wykonawca zapewni bezpłatną pomoc w instalacji udostępnianych przez producenta uaktualnień, poprawek oraz nowych wersji oprogramowania;
- 2) Wykonawca zapewni wsparcie/opiekę w zakresie obsługi dostarczonego oprogramowania zarządzającego przez 40 roboczogodzin w czasie trwania umowy gwarancyjnej. Zakres usługi będzie każdorazowo szczegółowo określany w ramach zgłoszeń składanych Koordynatorowi Wykonawcy przez Koordynatorów Zamawiającego.

3.14. Wymagania bezpieczeństwa dla zaoferowanego oprogramowania do zarządzania Urządzeniami wielofunkcyjnymi:

- 1) Wykonawca musi szczegółowo określić niezbędne do działania rozwiązania wymagania w zakresie infrastruktury sieciowej i systemowej stosując zasadę przyznawania minimalnych, potrzebnych do poprawnej pracy uprawnień (np. wymagania w zakresie

- komunikacji sieciowej z dokładnością po portów TCP/UPD, uprawnienia do usług katalogowych Active Directory PSG sp. z o.o.).
- 2) Zabezpieczenia, które są dopuszczone do stosowania w oferowanym rozwiązaniu i połączeniach do niego muszą uwzględniać wersje protokołów, które w momencie projektowania aplikacji są powszechnie uznawane za bezpieczne.
 - 3) Zamawiający nie dopuszcza możliwości instalowania żadnych zabezpieczeń fizycznych w postaci kart, kluczy USB, fizycznych sieciowych serwerów licencyjnych.
- 3.15.** Zamawiający zastrzega sobie prawo nadzoru i uczestnictwa w procesie instalacji Systemu. Wykonawca dostarczy procedury/instrukcje instalacji i konfiguracji dla wszystkich komponentów Systemu.
- 3.16.** Wspierane systemy operacyjne środowiska serwera: aplikacja serwerowa musi być kompatybilna z Windows Server w wersji 2022 oraz nowszym. Jeżeli Wykonawca stosuje w oferowanym rozwiązaniu komponenty innych producentów wszystkie dostarczone i zastosowane komponenty muszą być kompatybilne i oficjalnie wspierane przez producenta danego oprogramowania dla Windows Server w wersji 2022 oraz nowszym.
- 3.17.** Wymagania odnośnie aplikacji WEB (jeżeli wymaga do obsługi oferowanego rozwiązania):
- 1) Nie może korzystać z komponentów ActiveX i wtyczek NPAPI,
 - 2) Kod wynikowy strony musi poprawnie działać z aktualną wersją Microsoft Edge,
 - 3) Nie może wykorzystywać Flasha, Silverlighta, apletów Java ani innej technologii klienckiej, która nie jest natywnie wspierana przez standardy W3C w przeglądarkach.
 - 4) Całość komunikacji sieciowej pomiędzy klientem (aplikacją kliencką, przeglądarką WEB lub klientem zdalnej konsoli) a serwerem musi być szyfrowana za pomocą protokołów/algorytmów uznawanych obecnie za bezpieczne.
- 3.18.** Systemy operacyjne, bazy danych oraz wszystkie komponenty systemowe muszą umożliwiać instalację poprawek oraz nowych wersji udostępnianych przez ich producenta (w szczególności dotyczących bezpieczeństwa). Wykonawca w ramach dostarczonej gwarancji na System musi niezwłocznie po udostępnieniu aktualizacji bezpieczeństwa dla systemu operacyjnego, bazy danych lub komponentu Systemu dostosować System do poprawnej współpracy z tą aktualizacją oraz dostosować System do poprawnej współpracy z tą wersją.
- 3.19.** Wszystkie dostarczane Urządzenia muszą współpracować z Systemem, który będzie równoważny z posiadanym przez Zamawiającego oprogramowaniem SafeCom.
- 3.20.** Wykonawca zobowiązuje się dostarczyć wymagane licencje Systemu oraz przeprowadzić bezprzerwowe (utrzymanie ciągłości wydruku urządzeń w ramach godzin pracy u Zamawiającego) podłączenie obecnie posiadanych przez Zamawiającego urządzeń wielofunkcyjnych, do oferowanych rozwiązań o równoważnej funkcjonalności, w tym umożliwić dostęp do nich poprzez posiadane przez Zamawiającego karty HID ICLASS Seos+Prox, MIFARE ,UNIQUE.
- 3.21.** Przez System równoważny z posiadanym przez Zamawiającego oprogramowaniem SafeCom rozumie się oprogramowanie spełniające wymagania określone w Załączniku nr 2 do Umowy oraz tak jak dla oprogramowania SafeCOM w pkt. 3.22-3.27 poniżej.
- 3.22.** Wszystkie dostarczane Urządzenia muszą poprawnie wystawiać dane o stanie materiałów eksploatacyjnych oraz współpracować z posiadanym przez Zamawiającego oprogramowaniem Sprint Capture (SPC-FM) aplikacja do monitoringu urządzeń, stanu materiałów eksploatacyjnych.
- 3.23.** Wszystkie dostarczone Urządzenia muszą być wyposażone w czytnik wielosystemowy MultiReader dla kart zbliżeniowych obsługujący co najmniej standardy: HID ICLASS Seos+Prox, MIFARE i UNIQUE.
- 3.24.** Dla Urządzeń wielofunkcyjnych czytnik kart ma być podłączony bezpośrednio do Urządzenia z wykorzystaniem portu USB. Montaż czytnika kart zbliżeniowych nie może powodować utraty gwarancji Urządzenia.
- 3.25.** Czytnik kart zbliżeniowych musi być zasilany bezpośrednio z Urządzenia bez konieczności zasilania zewnętrznego oraz bez dodatkowego adresu IP.

3.26. Wszystkie posiadane przez Zamawiającego Urządzenia wielofunkcyjne podłączone do systemu oraz Urządzenia dostarczane w ramach przedmiotu Zamówienia muszą być obsługiwane przez jeden uniwersalny sterownik wydruku oraz poprawnie działać w środowisku Zamawiającego. W tym celu Zamawiający może dostarczyć i zapewnić możliwość korzystania z oprogramowania uniwersalnego sterownika.

3.27. W ramach realizacji przedmiotu umowy Wykonawca zobowiązany jest do podłączenia i konfiguracji dostarczonych Urządzeń do dostarczonego Systemu. Podstawowe założenia:

- 1) podłączenie dostarczonych Urządzeń wielofunkcyjnych do Systemu.
- 2) instalacja i konfiguracja czytników kart zbliżeniowych,
- 3) instalacja oprogramowania sterującego pracą czytnika na Urządzeniach,
- 4) sprawdzenie poprawności konfiguracji każdego Urządzenia (wydruku podążającego PULL Printing, skanowania do e-mail, skanowania do folderu),
- 5) sprawdzenie poprawności zliczania stron w Systemie.

Wymagania i wdrożenie oprogramowania równoważnego w zakresie SafeCom.

1. Przedmiot wdrożenia.

Przedmiotem wdrożenia jest dostawa, oraz uruchomienie systemu wydruku podążającego w infrastrukturze Zamawiającego, obejmujące:

- 1.1. Dostawa niezbędnych licencji wieczystych.
- 1.2. Instalacja i konfiguracja systemu, w tym integracja z istniejącą infrastrukturą IT (serwery, **drukarki**, konta użytkowników).
- 1.3. Testy akceptacyjne i optymalizacja ustawień.
- 1.4. Dokumentacja powdrożeniowa.
- 1.5. Warsztaty dla administratorów.
- 1.6. Wsparcie powdrożeniowe.

Wykonawca zobowiązuje się zrealizować wdrożenie w terminie **9 miesięcy** od daty podpisania umowy.

2. Wymagania funkcjonalne dla systemu równoważnego z SafeCom.

System powinien zapewniać m.in.:

- 2.1. Współpraca z drukarkami wielu producentów w wydruku podążającym (1500 szt.) – wsparcie dla urządzeń różnych marek obecnych u Zamawiającego zgodnie z listą poniżej:

HP Color LaserJet CM3530 MFP
HP Color LaserJet flow MFP M880
HP Color LaserJet MFP M577
HP LaserJet 500 color MFP M575
HP LaserJet 700 color MFP M775
HP LaserJet MFP M527
HP LaserJet MFP M725
KONICA MINOLTA bizhub 554e
KONICA MINOLTA bizhub C308
KONICA MINOLTA bizhub C3850
KONICA MINOLTA bizhub C3851
KONICA MINOLTA bizhub C450i
KONICA MINOLTA bizhub C454e
KONICA MINOLTA bizhub C458
KONICA MINOLTA bizhub C550i
RICOH Aficio MP C2050
RICOH Aficio MP C2051
RICOH Aficio SP 5200S
RICOH MP C3003
RICOH MP C3004

RICOH MP C3004ex
RICOH MP C401
Xerox AltaLink C8035 Multifunction Printer
Xerox AltaLink C8045 Multifunction Printer
Xerox AltaLink C8055 Multifunction Printer
Xerox AltaLink C8135 Multifunction Printer
Xerox AltaLink C8155 Multifunction Printer
Xerox VersaLink C405 DN Multifunction Printer
Xerox VersaLink C505 X Multifunction Printer
Xerox VersaLink C605 X Multifunction Printer
Xerox VersaLink C7020 Multifunction Printer
Xerox VersaLink C7030 Multifunction Printer
Xerox WorkCentre 7125 v 5. 12. 0 Multi System

W przypadku modeli urządzeń, które nie współpracują z zaproponowanym systemem mogą zostać dostarczone w ramach oferty Urządzenia o podobnych, nie gorszych parametrach technicznych, które będą kompatybilne z systemem poprzez terminal embedded. Zaproponowane Urządzenia muszą pochodzić od producentów urządzeń wykorzystywanych już u Zamawiającego.

System powinien również zapewnić obsługę drukarek w wydruku bezpośrednim w zakresie zliczania ilości wydruków.

- 2.2.** Obsługa minimalnie 11000 użytkowników w 260 lokalizacjach.
- 2.3.** Konsola administracyjna umożliwiająca szybki podgląd ilości użytkowników, urządzeń, serwerów infrastruktury.
- 2.4.** Możliwość logowania się do konsoli administracyjnej za pomocą poświadczeń domeny Windows.
- 2.5. Drukowanie i skanowanie:**
 - 2.5.1. Możliwość wysłania wydruku do wspólnej kolejki i odebrania go na dowolnym Urządzeniu po uwierzytelnieniu.
 - 2.5.2. Możliwość definiowania funkcji forsowania wydruku dwustronnego dla wybranych urządzeń lub grup użytkowników.
 - 2.5.3. Możliwość włączenia/wyłączenia domyślnego wydruku monochromatycznego,
 - 2.5.4. Automatyczne kasowanie oczekujących wydruków po czasie określonym przez Zamawiającego.
 - 2.5.5. System powinien posiadać opcję delegacji wydruków.
 - 2.5.6. Możliwość włączenia opcji przyzwolenia na zachowywanie wydruków, które nie będą automatycznie usuwane.
 - 2.5.7. Możliwość zamaskowania kodu ID podczas wpisywania na Urządzeniu.
 - 2.5.8. Wysyłanie zeskanowanych prac do skrzynki e-mail z opcją wyboru do aktualnie zalogowanego użytkownika.
- 2.6. Urządzenia:**
 - 2.6.1. Możliwość podglądu podstawowych danych o Urządzeniu.
 - 2.6.2. Możliwość zdefiniowania/edycji nazwy Urządzenia, lokalizacji, adresu IP.
 - 2.6.3. Konsola administracyjna umożliwiająca konfigurowanie nazwy grupy architektury, adresów serwerów z jakimi Urządzenie ma się łączyć.
 - 2.6.4. Konsola administracyjna umożliwiająca konfigurowanie metody logowania do urządzeń.
- 2.7. Użytkownicy:**
 - 2.7.1. Konsola administracyjna umożliwiająca wyświetlanie informacji o loginie, ID kodach.

- 2.7.2. Konsola administracyjna umożliwiająca zarządzanie przypisanymi kodami.
- 2.7.3. System powinien zapewnić złożoność kodów ID, zgodnie z wymaganiami bezpieczeństwa IT.
- 2.7.4. Konsola administracyjna umożliwiająca ręczne dodanie użytkownika z informacjami o: login, imię i nazwisko, organization unit(departament), e-mail, kod kosztowy.
- 2.7.5. Możliwość przydzielania limitów i uprawnień do drukowania i kopiowania (kolor, mono), e-maila, skanowania oraz do przycisku zezwalającego na wydruk wszystkich dokumentów.
- 2.7.6. Możliwość ustalenia poziomu uprawnień użytkownika.
- 2.7.7. Możliwość zaimportowania i eksportowania zbiorczego do/z pliku wsadowego użytkowników, kodów logowania.

2.8. Uwierzytelnianie na Urządzeniach:

- 2.8.1. Kartą zbliżeniową (HID ICLASS Seos+Prox, MIFARE, UNIQUE).
- 2.8.2. Unikalnym ID kodem.
- 2.8.3. Oraz/lub loginem i hasłem domeny Windows.
- 2.8.4. Auto wylogowanie użytkownika po określonym czasie bezczynności.

2.9. Integracja z Active Directory / LDAP:

- 2.9.1. Wymagana synchronizacja kont użytkowników i grup.
- 2.9.2. Automatyczne generowanie ID kodu dla nowych użytkowników i wysyłanie ich mailem bez angażowania pracowników IT.

2.10. Raportowanie:

- 2.10.1. Generowanie raportów przetworzonych stron/zadań, aktywności użytkowników, urządzeń i kosztów poprzez wykorzystanie wbudowanych, gotowych szablonów raportów oraz parametryzację raportów między innymi:
 - 2.10.1.1. z podziałem na: działy i/lub departamenty, Urządzenia, projekty, użytkowników,
 - 2.10.1.2. z podziałem na rodzaj usługi: drukowanie monochromatyczne/kolorowe, jednostronne/dwustronne, kopiowanie monochromatyczne/kolorowe, jednostronne/dwustronne, skanowanie,
 - 2.10.1.3. na zadany okres czasu: dzień, miesiąc, rok,
 - 2.10.1.4. możliwość ustawienia spersonalizowanych okresów generowania raportów,
 - 2.10.1.5. możliwość raportowania kosztów.
- 2.10.2. Generowanie raportów zarówno w formacie graficznym jak i tekstowym, w formatach CSV i PDF.
- 2.10.3. Możliwość nadawania uprawnień do funkcji generowania raportów.

2.11. Portal samoobsługowy dla użytkowników:

- 2.11.1. Funkcjonalność zarządzania osobistą kolejką wydruków dla wszystkich użytkowników Systemu w zakresie:
 - 2.11.1.1. możliwości przejrzania listy wydruków, wyboru konkretnej pracy, zlecenia jej druku lub usunięcia,
 - 2.11.1.2. generowania ID kodów,
 - 2.11.1.3. możliwości włączenia opcji przyzwolenia na zachowywanie wydruków, które nie będą automatycznie usuwane.
- 2.11.2. Logowania za pomocą poświadczeń Windows (SSO).

2.12. Architektura:

- 2.12.1. Zapewnienie wysokiej dostępności systemu drukowania (serwery druku i bazy danych).
- 2.12.2. Wprowadzenie zmian w konfiguracji (kont użytkowników, urządzeń, schematów kosztowych) musi być automatycznie aplikowane na inne serwery.
- 2.12.3. W przypadku awarii połączenia pomiędzy serwerem w lokalizacji a serwerem centralnym użytkownicy w danej lokalizacji gdzie jest lokalny serwer muszą mieć

możliwość korzystania z systemu druku w pełnej funkcjonalności a zwłaszcza autoryzacji na Urządzeniach, drukowania, obierania wydruków, skanowania i kopiowania.

2.12.4. Aplikacja embedded:

- 2.12.4.1. Wspiera mechanizm failover,
- 2.12.4.2. Wspiera szyfrowanie symetryczne i asymetryczne,
- 2.12.4.3. Wspiera niestandardowe ustawienia SNMP v1, v2, v3,
- 2.12.4.4. Możliwość wskazania metody logowania (kod ID + karta),
- 2.12.4.5. Możliwość maskowania kodu ID podczas autoryzacji na Urządzeniu,
- 2.12.4.6. Możliwość ustawienia śledzenia po drukowaniu,
- 2.12.4.7. Ustawienie języka polskiego w aplikacji na Urządzeniu,
- 2.12.4.8. Automatyczne podstawianie adresu email zalogowanego użytkownika.

2.13. Notyfikacja:

- 2.13.1. System umożliwia wysyłanie maili z informacjami administracyjnymi.
- 2.13.2. System umożliwia wysyłanie maili do użytkownika związanych z rejestracją karty oraz informacji związanych z pracami.
- 2.13.3. Administrator ma możliwość tworzenia własnych szablonów wiadomości.

3. Wymagania funkcjonalne w zakresie współpracy z systemem SPCFM

SPCFM (SPrintCapture Fleet Meter) to oprogramowanie wdrożone u Zamawiającego do zarządzania rozproszoną flotą urządzeń drukujących, obsługi umów serwisowych na Urządzenia drukujące (zgłoszenia napraw i konserwacji), monitorowania wykorzystania drukarek jak i aktualnego stanu zużycia materiałów eksploatacyjnych w poszczególnych Urządzeniach.

3.1. Możliwość weryfikacji:

- 3.1.1. zainstalowanej na Urządzeniu wersji agenta systemu wydruku podążającego,
- 3.1.2. przynależności Urządzenia do serwera wydruku.

Zamawiający do ww. weryfikacji dopuszcza dowolne mechanizmy komunikacji.

4. Wymagania funkcjonalne w zakresie współpracy z systemem ZPD Report lub istniejącej funkcjonalności w zaproponowanym systemie.

4.1. Portal samoobsługowy dla użytkowników:

- 4.1.1. musi udostępniać zestawienie użytkownikowi dotyczące jego własnych przetworzonych wydruków i kopii,
- 4.1.2. musi udostępniać zestawienie kierownikom, dotyczące przetworzonych wydruków i kopii przez podległych im pracowników na podstawie struktury organizacyjnej w AD.

5. Wymagania techniczne

Zgodnie z **Załącznikiem nr 3 do Umowy: Wymagania techniczne.**

6. Wymagania bezpieczeństwa

Zgodnie z **Załącznikiem nr 4 do Umowy: Wymagania bezpieczeństwa.**

7. Licencje:

7.1. Wykonawca dostarczy licencje na System .

- 7.1.1. Licencja musi umożliwiać dodanie dowolnej liczby użytkowników.

7.2. Wykonawca dostarczy licencje dla aktualnie eksploatowanych urządzeń wielofunkcyjnych u Zamawiającego na:

- 7.2.1. Urządzenia dla wydruku podążającego - 1500 szt. ,
- 7.2.2. Urządzenia dla zliczania wydruków – Nielimitowane ,
- 7.2.3. wydruk podążający – 1500 szt.,

- 7.2.4. szczegółowe reguły wydruku – 1500 szt.,
- 7.2.5. rejestrację wszystkich informacji o aktywności, aż do poszczególnych zadań i użytkowników – 1500 szt.,
- 7.2.6. podpięcie wszystkich rodzajów czytników kart zbliżeniowych używanych obecnie w Systemie – 1500 szt. .
- 7.3. Licencja na Urządzenie drukujące musi być możliwa do wykorzystania na innym Urządzeniu również innego producenta.

8. Instalacja i konfiguracja systemu

- 8.1. Wykonawca dostarczy, zainstaluje i skonfiguruje System, który będzie spełniał wymagania funkcjonalne, techniczne i bezpieczeństwa:
 - 8.1.1. We współpracy z Zamawiającym przygotuje procedurę instalacji, parametryzacji oraz konfiguracji każdego modelu z urządzeń Zamawiającego.
- 8.2. Instalacja i konfiguracja Systemu na infrastrukturze Zamawiającego dotyczy dwóch niezależnych środowisk:
 - 8.2.1. produkcyjnego,
 - 8.2.2. testowego – środowisko zawierające minimalną ilość serwerów ale będące reprezentatywną instalacją dla środowiska produkcyjnego; każda funkcjonalność Systemu musi zostać zaimplementowana w środowisku testowym.
- 8.3. Wykonawca w terminie 14 dni roboczych od zawarcia Umowy przekaże Zamawiającemu do zatwierdzenia harmonogram wdrożenia.
- 8.4. Wykonawca przed przystąpieniem do prac wdrożeniowych przedstawi i uzgodni z Zamawiającym projekt techniczny:
 - 8.4.1. Projekt techniczny zawierać ma w szczególności opis instalacji Systemu, jego konfiguracji (serwery, bazy danych, tabele ruchu sieciowego), w tym integracji z istniejącą infrastrukturą IT (drukarki, konta użytkowników).
- 8.5. Wykonawca zobowiązuje się zrealizować wdrożenie w terminie **9 miesięcy** od daty podpisania umowy.

9. Testy akceptacyjne i optymalizacja ustawień:

- 9.1. Wykonawca w terminie 14 dni roboczych od zawarcia Umowy przekaże Zamawiającemu do zatwierdzenia plan testów funkcjonowania Systemu wydruku podążającego oraz testów bezpieczeństwa, który obejmował będzie dokładny opis poszczególnych testów oraz ich harmonogram.
- 9.2. Wykonawca zobowiązany jest do opracowania scenariuszy i przypadków testowych zgodny z QAC.
- 9.3. Wykonawca przeanalizuje i uzgodni z Zamawiającym zakres oraz specyfikę poszczególnych testów tak, aby zrealizowane testy pokryły wymagania wynikające z oczekiwań Zamawiającego. W szczególności testy funkcjonalne mają potwierdzić poprawność działania wszystkich urządzeń obecnie działających u Zamawiającego.
- 9.4. Testy muszą być wykonane pod nadzorem Zamawiającego.
- 9.5. Wykonawca wytworzy dokumentację (raport z wykonanych testów) uwzględniającą wykonywane czynności oraz wyniki działań w ramach wykonanych testów.
- 9.6. Testy zostaną zakończone z chwilą podpisania przez Zamawiającego protokołu odbioru testów.

10. Dokumentacja powdrożeniowa

- 10.1. Dokumentacja powykonawcza ma zawierać między innymi:
 - 10.1.1. opis techniczny docelowej architektury,
 - 10.1.2. opis Sytemu oraz jego parametryzację (konfiguracja, mechanizmy transmisji, szyfrowanie transmisji, wykorzystywane konta techniczne: domenowe i lokalne),
 - 10.1.3. opis procedur wdrażania i administrowania Systemem, w tym procedurę konfiguracji i podłączania nowych urządzeń,
 - 10.1.4. procedurę instalacji Systemu umożliwiającą jego odtworzenie po ewentualnej awarii,
 - 10.1.5. procedury awaryjne pozwalające na kontynuowanie drukowania, kopiowania i skanowania w przypadkach:
 - 10.1.5.1. niedostępności łączы pomiędzy Lokalizacjami,

- 10.1.5.2. braku łączności z najbliższym serwerem wydruku,
- 10.1.5.3. braku łączności z serwerem bazodanowym,
- 10.1.5.4. braku łączności z serwerem aplikacyjnym.

11. Warsztaty administratorów

- 11.1.** Warsztaty dla max. 7 pracowników w terminie ustalonym z Zamawiającym w zakresie administrowania Systemem, tj. w szczególności:
 - 11.1.1. monitorowanie i weryfikacja logów systemowych dotyczących pracy Systemu,
 - 11.1.2. licencjonowanie,
 - 11.1.3. konfiguracja usług,
 - 11.1.4. zarządzanie rozliczeniami kosztów wydruku,
 - 11.1.5. zarządzanie zasadami, regułami i uprawnieniami,
 - 11.1.6. tworzenie i konfigurowanie raportów.
- 11.2.** Warsztaty prowadzone będą w dni robocze w godzinach 8-15.

12. Odbiór wdrożenia Systemu:

- 12.1.** Zakończenie wdrożenia zostanie potwierdzone protokołem odbioru.
- 12.2.** Protokół ma zawierać wszystkie ustalenia i zalecenia poczynione w trakcie odbioru. Po podpisaniu protokołu bez zastrzeżeń przez obie strony w dniu następnym rozpoczyna się okres wsparcia powdrożeniowego.

13. Wsparcie powdrożeniowe:

- 13.1.** Wykonawca zapewni wsparcie powdrożeniowe (telefoniczne/zdalne/on-site) przez okres minimum 12 miesięcy.
- 13.2.** Wykonawca zapewni dostęp do poprawek, aktualizacji, nowych wersji oprogramowania.
- 13.3.** Wykonawca zapewni wsparcie techniczne przy instalacji aktualizacji, poprawek, nowych wersji oprogramowania.
- 13.4.** Wykonawca zobowiązany będzie do usuwania Wad, Awarii i Usterek Systemu. Wadą w rozumieniu Umowy jest działanie Systemu w sposób niezgodny z dokumentacją, które wpływa w sposób istotny na wyniki lub na użyteczność Systemu, ale niebędące awarią (Wada), awarią – stan Systemu, w którym nie jest możliwa jego faktyczna eksploatacja lub nie są realizowane (czy też są realizowane wadliwie) podstawowe funkcje użytkowe (Awaria), a usterką – działanie Systemu w sposób niezgodny z dokumentacją, które nie wpływa w sposób istotny na wyniki, ani na użyteczność Systemu (Usterka).
- 13.5.** W ramach wsparcia powdrożeniowego Wykonawca zobowiązany będzie do świadczenia Zamawiającemu wsparcia w rozwiązywaniu problemów z utrzymaniem, konfiguracją i użytkowaniem funkcjonalności Systemu. Świadczenie to będzie realizowane w dni robocze w godzinach 8:00 – 16:00. W ramach wsparcia Strony uzgadniają, że:
 - 13.5.1.** Zamawiający będzie uprawniony do zgłaszania Wad, Awarii, Usterek na adres email lub telefonicznie na nr w Dni robocze w godzinach 8:00 – 16:00,
 - 13.5.2.** Wykonawca niezwłocznie, nie później jednak niż w terminie 4 godzin, potwierdza zgłoszenie. W przypadku braku potwierdzenia zgłoszenia przez Wykonawcę, termin na usunięcie Wady, Awarii lub Usterki zaczyna biec od upływu terminu na potwierdzenie zgłoszenia.
 - 13.5.3.** Czas usunięcia Wad, Awarii lub Usterek Systemu:
 - 13.5.3.1. Awarii – w terminie 24 godzin od godziny potwierdzenia zgłoszenia,
 - 13.5.3.2. Wad – w terminie 7 Dni roboczych od dnia potwierdzenia zgłoszenia,
 - 13.5.3.3. Usterek – w terminie 10 Dni roboczych od dnia potwierdzenia zgłoszenia.
 - 13.5.4.** Zamawiający określi odpowiedni poziom w zgłoszeniu,

13.5.5. Za moment usunięcia Wady, Awarii lub Usterki uważa się chwilę zawiadomienia o tym fakcie Zamawiającego, o ile Zamawiający nie zgłosi następnie zastrzeżeń co do sposobu funkcjonowania Systemu.

WYMAGANIA TECHNICZNE
Terminologia

Usługa AD – wykorzystywana w PSG usługa Active Directory (usługa katalogowa) przechowująca informacje o kontach użytkowników, grupach oraz komputerach dodanych do domeny.

CPD – Centrum Przetwarzania Danych.

Wymagania względem Systemu**Wymagania techniczne**

- T1.** Planowany System ma być systemem centralnym wykorzystywanym przez użytkowników PSG, użytkowników Firm zewnętrznych.
- T2.** Konstrukcja Systemu musi zapewniać redundancje poszczególnych elementów, tak aby awaria któregośkolwiek z nich nie powodowała braku dostępności Systemu lub części funkcjonalności.
- T3.** System musi być odporny na awarię dowolnego komponentu, w tym całego, dowolnego serwera wirtualnego (np. aplikacyjnego czy bazy danych) w CPD podstawowym. Musi być zapewniona redundancja wszystkich komponentów w CPD podstawowym i awaria pojedynczego komponentu nie może wymagać przełączenia obsługi użytkowników do CPD zapasowego.
- T4.** Budowany System będzie składał się z dwóch rozproszonych geograficznie instancji (po jednej w CPD podstawowym i CPD zapasowym), zlokalizowanych w strategicznych Centrach Przetwarzania Danych Polskiej Spółki Gazownictwa. W trakcie normalnej pracy jedna instancja będzie aktywna (w jednym Centrum Przetwarzania Danych) tj. architektura Active-Pasive. W przypadku awarii jednej z instancji (np. jej kluczowych komponentów lub całego Centrum Przetwarzania Danych), druga musi w sposób niezauważony dla użytkownika przejąć funkcję obsługi całości użytkowników oraz dostarczać/prezentować wszystkie dane przetwarzane w Systemie. W ramach każdej z instancji (tj. instalacji w danym CPD) należy stosować mechanizmy zapewniające wysoką dostępność w ramach tej instancji (tj. mechanizmy klastrowe dla baz danych, rozkładanie obciążenia pomiędzy kilka serwerów aplikacyjnych). Wymagane jest aby w żadnym z CPD nie było pojedynczych punktów awarii (ang. Single point of failure (SPOF)).
- T5.** Wykonawca musi dostarczyć licencje dla Systemu i jego komponentów pozwalająca na migrację komponentów pomiędzy różne centra Przetwarzania Danych i różne klastry wirtualizacji bez ograniczeń co do wielkości tych klastrów (ilość i konfiguracja serwerów fizycznych).
- T6.** W ramach Systemu należy stosować mechanizmy zapewniające wysoką dostępność w szczególności mechanizmy klastrowe z wykorzystaniem wirtualizacji. Dostarczone licencje muszą pozwalać na dowolne przenoszenie dowolnych maszyn wirtualnych Systemu pomiędzy hostami i klastrami wirtualizacji. Rozwiązanie musi wspierać wirtualizację VMware vSphere w jej aktualnej wersji (min 8.0 i nowsze).
- T7.** W skład rozwiązania muszą wchodzić mechanizmy zapewniające wysoką wydajność dla wszystkich komponentów budowanego Systemu, w szczególności dla serwerów aplikacji, web oraz baz danych. Zamawiający dopuszcza stosowanie pojedynczego serwera bazy danych i wymaga stosowania więcej niż jednego serwera aplikacyjnego/serwera web. Zamawiający wymaga aby System umożliwiał skalowanie wydajności poprzez dodanie kolejnych serwerów aplikacyjnych/web. Wymagane jest aby całkowite obciążenie serwera bazy danych nie przekraczało 20% mocy obliczeniowej wymaganej dla całego Systemu (podział obciążenia do 20% - serwer bazy danych, około 80% - serwery aplikacyjne/web).

- T8.** Rozkładanie obciążenia pomiędzy serwery aplikacyjne i serwery web realizowane będzie za pomocą stosowanych u Zamawiającego loadbalancerów pracujących w trybie full proxy z mechanizmem SSL Offload/SSL Acceleration. Wymagane jest, aby Wykonawca dopasował System do poprawnej współpracy ze stosowanym u Zamawiającego rozwiązaniem w tym zakresie. W przypadku, jeżeli System wymagał będzie persystencji sesji (ang. session persistence lub stickiness) dopuszczalna metoda zachowania persystencji to wykorzystanie http cookie (ang. Cookie Persistence).
- T9.** System musi być skalowalny tj. zapewnić możliwość rozbudowy o dodatkowe serwery bez konieczności zmian programistycznych. Konstrukcja systemu powinna pozwalać na elastyczne skalowanie.
- T10.** Wymagane jest aby Wykonawca dopasował rozwiązanie do poprawnej współpracy ze stosowanym u Zamawiającego rozwiązaniem informatycznym SPCFM.
- T11.** W przypadku stosowania aplikacji web, web-api oraz komunikacji za pomocą protokołu http pomiędzy komponentami systemu oraz w komunikacji z przeglądarką Użytkowników wymagane jest stosowanie protokołu HTTP/2 lub jego nowszej wersji. System dla kompatybilności musi umożliwiać połączenia również za pomocą protokołu HTTP/1.1.
- T12.** Stosowane serwery WEB (w przypadku stosowania aplikacji web lub web-api) muszą obsługiwać i komunikować się za pomocą protokołów HTTP/2 lub jego nowszej wersji. System dla kompatybilności musi umożliwiać połączenia również za pomocą protokołu HTTP/1.1.
- T13.** System musi poprawnie działać przy wymuszonych przez WAF nagłówkach HTTP o wartościach jak niżej:
- a. X-Frame-Options o wartości: SAMEORIGIN
 - b. X-Content-Type-Options o wartości: nosniff
 - c. X-XSS-Protection o wartości: 1; mode=block
 - d. Referrer-Policy o wartości: same-origin
 - e. Strict-Transport-Security o wartości: max-age=31536000; includeSubDomains; preload
 - f. Server o wartości: PSG
 - g. Expect-CT o wartości: enforce, max-age=30
- T14.** System będzie obsługiwał Użytkowników i przetwarzał dane z systemów/aplikacji rozmieszczonych na terenie całej Polski za pośrednictwem sieci Zamawiającego oraz sieci Internet. Wobec powyższego Zamawiający wymaga od Wykonawcy określenia obciążenia ruchu sieciowego na poziomie sieci WAN i sieci Internet (wymagane pasmo w rozbiciu na per użytkownik, per obsługiwany system/aplikację oraz inny ruch jeżeli wymagany do pracy Systemu) i zdefiniowania ruchu sieciowego koniecznego do działania aplikacji.
- T15.** System ma wykorzystywać aktualną wersję relacyjnej bazy danych: Microsoft SQL Enterprise w wersji 2022 lub nowszej. Wymagane jest stosowanie aktualnej wersji stabilnej na dzień instalacji Systemu udostępnionej przez producenta (Microsoft). Wykonawca będzie dopasowywał System do udostępnianych przez producenta aktualnych wersji lub poprawek dla danej wersji w terminie maksymalnie 12 miesięcy od udostępniania nowej wersji oraz w terminie maksymalnie 1 tygodnia od udostępnienia aktualizacji bezpieczeństwa.
- T16.** Wymagane są wydzielone min. 2 środowiska: produkcyjne i testowe/rozwojowe:
- Testowe (TST)
 - Produkcyjne (PRD)
- T17.** Systemy PRD i TST nie mogą współdzielić żadnych zasobów i komponentów (wymagana całkowita separacja środowisk).

- T18.** System testowy musi być zbudowany w architekturze identycznej jak środowisko produkcyjne.
- T19.** Zamawiający zapewnia infrastrukturę techniczną (w tym licencje bazodanowe) wymaganą do uruchomienia Systemu. Wykonawca przy współpracy z Zamawiającym określi wymagania dotyczące środowiska sprzętowego, tak żeby System był bezpieczny, wydajny i stabilny, przy czym na potrzeby realizacji projektu Zamawiający dostarczy środowisko w postaci maszyn wirtualnych VMware vSphere o sumarycznej ilości zasobów: 256GB pamięci operacyjnej (vRAM), 128 procesorów wirtualnych (vCPU) oraz 1 TB przestrzeni dyskowej (vDISK) na dyskach SSD i 2 TB przestrzeni dyskowej (vDISK) na dyskach magnetycznych. Pojedyncza maszyna wirtualna nie może wymagać więcej niż 32 GB vRAM i 16 vCPU. Sumaryczna ilość zasobów serwerowych wymaganych do poprawnej i wydajnej pracy Systemu nie może przekraczać określonych w tym punkcie wartości maksymalnych, przy czym Zamawiający dopuszcza dowolny podział zasobów pomiędzy poszczególne maszyny wirtualne, zgodnie z oczekiwaniami Wykonawcy.
- T20.** Serwery - standardem są serwery jako maszyny wirtualne działające w środowisku VMware vSphere w jego aktualnej wersji. Wykonawca określa w Projekcie Technicznym wymagane parametry konfiguracyjne poszczególnych maszyn wirtualnych oraz ich ilość:
- vRAM
 - vCPU
 - vDISK
- T21.** Zamawiający nie dopuszcza do instalacji maszyn wirtualnych lub kontenerów z gotowych obrazów (OVF, OVA, kontenery lub inne).
- T22.** Zamawiający nie dopuszcza do instalacji środowiska w postaci kontenerów (np. Docker).
- T23.** Zamawiający nie dopuszcza możliwości instalowania żadnych zabezpieczeń fizycznych w postaci kart, kluczy USB, fizycznych sieciowych serwerów licencyjnych.
- T24.** Zamawiający zastrzega sobie prawo nadzoru i uczestnictwa w procesie instalacji Systemu. Wykonawca dostarczy procedury/instrukcje instalacji i konfiguracji dla wszystkich komponentów Systemu.
- T25.** System musi być zbudowany w architekturze trójwarstwowej:
- warstwa bazy danych (serwery baz danych)
 - warstwa logiki aplikacji (serwery aplikacyjne)
 - warstwa prezentacji (aplikacje klienckie)
- T26.** Aplikacje klienckie nie mogą komunikować się bezpośrednio z bazą danych.
- T27.** Wspierane systemy operacyjne środowiska serwera: aplikacja serwerowa musi być kompatybilna z jednym z wymienionych systemów operacyjnych: Windows Server w wersji 2022 lub nowszej, Red Hat Enterprise Linux w wersji 9 lub nowszej. Jeżeli Wykonawca stosuje w Systemie komponenty innych producentów wszystkie dostarczone i zastosowane komponenty muszą być kompatybilne i oficjalnie wspierane przez producenta danego oprogramowania na jednym z wymienionych systemów operacyjnych: Windows Server w wersji 2022 lub nowszej, Red Hat Enterprise Linux w wersji 9 lub nowszej.
- T28.** Zamawiający zapewnia licencję na system operacyjny: Windows Server Datacenter, Red Hat Enterprise Linux oraz silnik bazy danych: MS SQL Enterprise. Jeżeli system wymaga innych komponentów wymagane jest dostarczenie przez Wykonawcę wszystkich licencji objętych komercyjnym wsparciem technicznym producenta na okres trwania gwarancji technicznej na budowany System.

- T29.** Wymagane jest, aby wszystkie wykorzystane przez Wykonawcę komponenty firm trzecich dostarczone i wykorzystane były w oficjalnej wersji udostępnianej przez Producenta danego komponentu oficjalnym kanałem dystrybucji jego oprogramowania. Nie jest dopuszczalne stosowanie komponentów lub bibliotek firm trzecich w postaci tzw. selfbuild lub self-compiled. Wymagane jest, aby Wykonawca wykorzystał najnowszą wersję stabilną (produkcyjną) danego komponentu oraz dopasował System do udostępnianych przez producenta aktualnych wersji lub poprawek dla danej wersji w terminie maksymalnie 12 miesięcy od udostępniania nowej wersji oraz w terminie maksymalnie 1 tygodnia od udostępnienia aktualizacji bezpieczeństwa. Wszystkie stosowane przez Wykonawcę w Systemie komponenty muszą być w wersji oficjalnie wspieranej i rozwijanej przez producenta danego komponentu.
- T30.** Zamawiający nie dopuszcza stosowania oprogramowania i komponentów Open Source, z wyjątkiem oprogramowania i komponentów Open Source dla których Wykonawca dostarczy komercyjne wsparcie ich producenta na czas gwarancji technicznej na dostarczony System. Zamawiający dopuszcza jednocześnie zastosowanie bibliotek Open Source, które nie będą objęte komercyjnym wsparciem pod warunkiem stosowania tych bibliotek w aktualnej wersji, oficjalnie udostępnionej przez Producenta lub społeczność bez znanych podatności. W przypadku wykrycia podatności technicznej w zastosowanej bibliotece Open Source, dla której społeczność lub Producent nie dostarczy w terminie 30 dni poprawki bezpieczeństwa obowiązkiem Wykonawcy będzie zastosowanie innej biblioteki bez znanych podatności w terminie maksymalnie 90 dni od oficjalnego ogłoszenia danej podatności technicznej. W przypadku dostępności danego komponentu lub biblioteki w oficjalnych, podstawowych repozytoriach systemu operacyjnego udostępnianych przez Producenta (Red Hat Enterprise Linux lub Windows Server) obowiązkiem Wykonawcy jest zastosowanie komponentu z oficjalnego repozytorium. Jednocześnie wszystkie komponenty dostępne w oficjalnym, podstawowym repozytorium Red Hat Enterprise Linux spełniając wymóg posiadania komercyjnego wsparcia Producenta, które dostarcza w tym wypadku Zamawiający w ramach subskrypcji na OS.
- T31.** Zamawiający nie dopuszcza stosowania oprogramowania i komponentów Open Source, które nie są oficjalnie rozwijane. W przypadku jeżeli w ramach danego projektu Open Source przez okres 1 roku nie wprowadzono zmian programistycznych, poprawek, nie wydano nowych wersji należy uznać, że komponent Open Source jest nierozwijany i nie można go zastosować.
- T32.** W przypadku zaprzestania rozwoju w zastosowanej bibliotece Open Source (brak zmian w projekcie przez okres 1 roku) obowiązkiem Wykonawcy będzie zastosowanie innej, rozwijanej biblioteki bez znanych podatności w terminie maksymalnie 90 dni od uznania danego komponentu jako nierozwijany. Aktualizacja musi być dostarczona bez dodatkowych opłat, w ramach gwarancji na dostarczone rozwiązanie.
- T33.** Zamawiający nie dopuszcza stosowania oprogramowania, komponentów, funkcji, technologii oficjalnie oznaczonych jako nierozwijane, przestarzałe lub w wersji oznaczonej jako nierozwijana/przestarzała.
- T34.** Wszystkie wykorzystywane w systemie komponenty i biblioteki firm trzecich (np. Java, serwery aplikacyjne) muszą być objęte komercyjnym wsparciem producenta danego oprogramowania na czas trwania gwarancji dla Systemu. Dostarczona licencja musi umożliwiać zgodne z warunkami licencyjnymi producenta danego komponentu korzystanie z tego oprogramowania przez wszystkich użytkowników Systemu oraz uwzględniać środowisko techniczne Zamawiającego, w

szczegółności wirtualizację serwerów i możliwość dowolnego przenoszenia maszyn wirtualnych pomiędzy klastrami wirtualizacji. W przypadku korzystania z komponentów firm trzecich Wykonawca przedstawi listę tych komponentów oraz koszt licencji i gwarancji technicznej dla nich na czas trwania gwarancji na System.

- T35.** Zamawiający wymaga aby wszystkie zastosowane w systemie komponenty i biblioteki były w aktualnej, najnowszej stabilnej wersji wydanej przez dostawcę danego komponentu (np. systemy operacyjne, bazy danych, serwery aplikacyjne oraz całe pozostałe programowanie i jego komponenty). Jeżeli producent danego komponentu oznacza poszczególne wersje stabilne jako objęte długoterminowym wsparciem (np. LTS) należy skorzystać z tej wersji.
- T36.** Wszystkie komponenty, aplikacje i usługi serwerowe muszą być uruchamiane jako usługi systemowe. Musi być zapewniony automatyczny start usług po restarcie Systemu Operacyjnego i poprawne uruchomienie wszystkich komponentów Systemu w przypadku restartu dowolnego z serwerów.
- T37.** Aplikacje klienckie muszą być typu 'cienki klient' i posiadać minimalne wymagania dla łącza przy pracy w sieci WAN. Aplikacja kliencka nie może łączyć się bezpośrednio z bazą danych. System nie powinien wykorzystywać jako aplikacji klienckiej połączenia RDP, Citrix lub innych metod zdalnego dostępu do serwera. Aplikacja kliencka musi być aplikacją WEB lub natywną aplikacją Windows. Dla Klientów PSG wymagane jest aby aplikacją kliencką była aplikacja WEB.
- T38.** Aplikacja kliencka nie może łączyć się bezpośrednio z bazą danych.
- T39.** Wymagania do aplikacji klienckiej:
- musi pracować w kontekście standardowego użytkownika Windows,
 - musi posiadać ergonomiczny interfejs użytkownika,
 - musi umożliwiać pełną obsługę błędów za pomocą jednoznacznych zrozumiałych komunikatów, bez wyświetlania informacji technicznych pozwalających na identyfikację zastosowanych technologii i bez zwracania informacji technicznych np. zapytań do baz danych lub podobnych,
 - aplikacja WEB:
 - nie może korzystać z komponentów ActiveX i wtyczek NPAPI
 - nie może wykorzystywać Flasha, Silverlighta, apletów Java ani innej technologii klienckiej, która nie jest natywnie wspierana przez standardy W3C w przeglądarkach.
 - warstwę prezentacji należy tworzyć wyłącznie w formacie HTML5 z użyciem CSS3.
 - kod wynikowy strony musi poprawnie działać z każdą z niżej wymienionych przeglądarek w ich aktualnej wersji:
 - Microsoft Edge,
 - Google Chrome na platformie MS Windows, Linux oraz macOS,
 - Safari na platformie macOS,
 - Mozilla Firefox na platformie MS Windows, Linux oraz macOS.
- T40.** Wymagane jest, aby Wykonawca dopasowywał w ramach gwarancji technicznej System do poprawnej współpracy z aktualną wersją stabilną w/w przeglądarek w miarę udostępnianych przez producenta aktualnych wersji lub poprawek dla danej wersji: w terminie maksymalnie 1 miesiąca od udostępniania nowej wersji oraz w terminie maksymalnie 1 tygodnia od udostępnienia aktualizacji bezpieczeństwa.
- T41.** Ruch sieciowy pomiędzy wszystkimi elementami systemu musi być szyfrowany za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Wymagane

jest stosowanie protokołów TLSv1.3 lub ich nowszych wersji. Nie jest dopuszczalne stosowanie protokołu IPsec oraz protokołów SSL 2.0, SSL 3.0, TLS 1.0 i TLS 1.1 i starszych. Stosowanie protokołu TLSv1.2 jest dopuszczalne tylko w szczególnie uzasadnionych przypadkach po akceptacji przez PSG takiego protokołu, przy czym nie jest dopuszczalne stosowanie protokołu TLSv1.2 do komunikacji z przeglądarką internetową użytkowników Systemu.

- T42.** Wymagane jest stosowanie protokołów, algorytmów oraz ich konfiguracji powszechnie uznanych za bezpieczne.
- T43.** Wymagane jest stosowanie zaufanych certyfikatów X.509 dostarczonych przez Zamawiającego. Stosowane muszą być certyfikaty z wewnętrznej infrastruktury PKI Zamawiającego lub certyfikaty komercyjne zakupione przez Zamawiającego. Wymagana, minimalna długość klucza dla ECC to 384 bitów, dla RSA to 2048 bitów.
- T44.** Nie dopuszcza się bezpośredniej komunikacji Systemu z innymi Systemami, aplikacjami i bazami danych. System będzie się komunikował z innymi Systemami Zamawiającego za pośrednictwem szyny danych.
- T45.** System ma być w całości posadowiony w infrastrukturze Zamawiającego (ang. on-premises). Nie jest dopuszczalne aby System lub jakikolwiek jego komponent wymagał komunikacji z elementami posadowionymi poza infrastrukturą zamawiającego (np. zewnętrzne serwery licencji).
- T46.** Żaden z serwerów oraz aplikacja kliencka nie mogą wymagać komunikacji z siecią Internet tj. komponentami posadowionymi poza infrastrukturą Zamawiającego przez sieć Internet.
- T47.** Wymagana jest separacja serwerów i komponentów Systemu publikowanych do sieci publicznej Internet od części Systemu obsługiwanej w sieci wewnętrznej. W części systemu publikowanej do sieci Internet nie może być dostępna funkcjonalność dla pracowników PSG, w szczególności moduły do zarządzania systemem. Część systemu publikowana do sieci Internet nie może zawierać kodu i funkcjonalności, która nie jest niezbędna dla obsługi użytkowników korzystających z fragmentu systemu udostępnionej do Internetu.
- T48.** System musi zapewniać integrację z wykorzystywanym przez Zamawiającego katalogiem Active Directory na potrzeby autoryzacji użytkowników. Część Systemu dla obsługi pracowników PSG musi integrować się z Active Directory w zakresie autentykacji użytkowników – pracowników PSG tj. musi korzystać z mechanizmu jednorazowego uwierzytelnienia (Single Sign-On) – dostęp do aplikacji bez pytania użytkownika o identyfikator lub hasło, uwierzytelniając użytkownika automatycznie za pomocą konta domenowego. W systemie nie mogą być przetwarzane lub przechowywane hasła dla kont pracowników PSG.
- T49.** Integracja z Active Directory: autentykacja do wszystkich elementów Systemu w tym również dla Administratorów musi być realizowana w oparciu o usługi katalogowe Active Directory.
- T50.** System musi wspierać SAML 2.0 (Security Assertion Markup Language 2.0) w szczególności w połączeniu z MS ADFS 5.0 i nowszym (Microsoft Active Directory Federation Services) w zakresie SSO dla użytkowników.
- T51.** System powinien zapewniać dystrybucję powiadomień, alertów i raportów poprzez e-mail i integrację z wykorzystywanym u Zamawiającego systemem pocztowym opartym o MS Exchange. Wymagana jest obsługa szyfrowanych za pomocą TLS w wersji min. 1.2 połączeń protokołem SMTP (protokół StartTLS).
- T52.** System powinien zapewniać weryfikowanie poprawności wprowadzonych danych poprzez możliwość konfiguracyjnego określania wymagalności pól wypełnianych przez użytkowników.

- T53.** System powinien mieć możliwość konfiguracji złożoności kodów dostępu do urządzeń drukujących, tak aby możliwa była edycja tej konfiguracji.
- T54.** System powinien dawać możliwość konfigurowania reguł walidacyjnych dla wprowadzanych danych.
- T55.** Instalacja Systemu przeprowadzona musi być lokalnie w jednej z siedzib PSG wskazanej przez Zamawiającego, wspólnie z administratorami PSG na podstawie przygotowanej przez Dostawcę instrukcji/procedury instalacji i konfiguracji.
- T56.** Zamawiający nie przewiduje dostępu zdalnego do systemu produkcyjnego dla pracowników Wykonawcy. Zmiany i poprawki do systemu produkcyjnego będą wgrywane przez pracowników Zamawiającego na bazie dostarczonych przez Wykonawcę procedur i instrukcji. Po uzgodnieniu z Zamawiającym dopuszczalne jest realizowanie części lub całości prac instalacyjnych zdalnie poprzez System wideokonferencyjny Zamawiającego i współdzielenie pulpitu z pracownikami Zamawiającego.
- T57.** Zamawiający nie przewiduje dostępu administracyjnego do żadnego z serwerów Systemu, w tym też dla serwerów testowych i deweloperskich.
- T58.** Każdy użytkownik Systemu musi posiadać indywidualne (imienne) konto, pozwalające na jego jednoznaczną identyfikację.
- T59.** Konfiguracje wszystkich komponentów w tym systemy operacyjne, bazy danych, serwery aplikacji i inne komponenty muszą podlegać procesowi optymalizacji działania i poprawy stanu zabezpieczeń (hardeningu) na podstawie zaleceń producentów wykorzystywanego oprogramowania, ogólnie uznanych za poprawne zasad i standardów bezpieczeństwa oraz ogólnodostępnymi benchmarkami np. CIS Benchmarks <https://www.cisecurity.org/cis-benchmarks/>. Wykonawca dostarczy szczegółowe wytyczne do utwardzania konfiguracji wszystkich elementów Systemu. W szczególności hardening powinien obejmować:
- a. instalację wyłącznie niezbędnych pakietów oprogramowania (lub usunięcie zbędnych),
 - b. określenie polityki haseł i polityki blokowania kont użytkowników,
 - c. instalację i uruchamianie wyłącznie niezbędnych usług sieciowych (lub wyłączenie zbędnych),
 - d. ustalenie restrykcyjnych praw dostępu do wszystkich krytycznych obiektów w Systemie,
 - e. parametry udostępnionych usług sieciowych,
 - f. usunięcie wszystkich znanych podatności technicznych wykrytych przez skanery podatności stosowane przez Zamawiającego.
- T60.** System musi być objęty systemem archiwizacji danych istniejącym u Zamawiającego. Musi być zapewnione wykonywanie kopii zapasowej: konfiguracji Systemu oraz przetwarzanych danych zgodnie z przyjętą w tym zakresie u Zamawiającego polityką backupu.
- T61.** Systemy operacyjne, bazy danych oraz wszystkie komponenty systemowe muszą umożliwiać instalację poprawek oraz nowych wersji udostępnianych przez ich producenta (w szczególności dotyczących bezpieczeństwa). Wykonawca w ramach dostarczonej gwarancji na System musi niezwłocznie tj. w terminie maksymalnie 1 tygodnia po udostępnieniu aktualizacji bezpieczeństwa dla systemu operacyjnego, bazy danych lub komponentu Systemu dostosować System do poprawnej współpracy z tą aktualizacją oraz w terminie maksymalnie 3 miesięcy od udostępniania nowej wersji lub innej aktualizacji dostosować System do poprawnej współpracy z tą wersją.
- T62.** Dostarczony system musi wspierać najnowszą wersję języka programowania, w którym został stworzony w ramach wersji jak i nowych pojawiających się linii wersji tego oprogramowania.

Wykonawca w ramach dostarczonej gwarancji na System musi niezwłocznie tj. w terminie maksymalnie 1 tygodnia po udostępnieniu aktualizacji bezpieczeństwa dostosować System do poprawnej współpracy z tą aktualizacją oraz w terminie maksymalnie 12 miesięcy od udostępniania nowej wersji lub innej aktualizacji dostosować System do poprawnej współpracy z tą wersją języka programowania.

- T63.** W przypadku wykorzystania w dostarczonym Systemie Java wymagane jest stosowanie aktualnej, najnowszej na dzień składania oferty wersji LTS (minimum Java 21 LTS) z aktualnymi poprawkami bezpieczeństwa. W przypadku instalacji na systemie operacyjnym RHEL wymagane jest stosowanie komponentów Java z systemowych repozytoriów Red Hat Enterprise Linux, w przypadku instalacji na Windows wymagane jest stosowanie komponentów Java wydanych przez Azul w wersji komercyjnej, gdzie Wykonawca dostarczy niezbędne licencje objęte wsparciem producenta na okres gwarancji technicznej na system. Zamawiający dopuszcza też zastosowanie wersji Community Java. Wykonawca w ramach dostarczonej gwarancji na System musi niezwłocznie tj. w terminie maksymalnie 1 tygodnia po udostępnieniu aktualizacji bezpieczeństwa dostosować System do poprawnej współpracy z tą aktualizacją oraz w terminie maksymalnie 12 miesięcy od udostępniania nowej wersji LTS dostosować System do poprawnej współpracy z tą wersją.
- T64.** W przypadku wykorzystania w dostarczonym Systemie .NET Framework lub .NET (core) wymagane jest stosowanie aktualnej wersji tj. min 4.8.1 .NET Framework lub .NET 8.0.5. Wykonawca w ramach dostarczonej gwarancji na System musi niezwłocznie tj. w terminie maksymalnie 1 tygodnia po udostępnieniu aktualizacji bezpieczeństwa dostosować System do poprawnej współpracy z tą aktualizacją oraz w terminie maksymalnie 12 miesięcy od udostępniania nowej wersji dostosować System do poprawnej współpracy z tą wersją.
- T65.** Oprogramowanie antywirusowe (dostarczone przez Zamawiającego) musi umożliwiać współpracę i być zainstalowane na wszystkich serwerach Windows i Linux oraz stacjach użytkowników (pracowników PSG).
- T66.** Wykonawca określi szczegółowo niezbędne do działania Systemu wymagania w zakresie infrastruktury sieciowej i systemowej stosując zasadę przyznawania minimalnych, potrzebnych do poprawnej pracy uprawnień (np. wymagania w zakresie komunikacji sieciowej z dokładnością po portów TCP/UDP, uprawnienia do usług katalogowych, uprawnień do baz danych).
- T67.** Dostarczone w ramach realizacji przedmiotu zamówienia materiały (np. projekt techniczny, dokumentacja powykonawcza) muszą być w języku polskim. Prowadzone szkolenia, warsztaty i spotkania robocze muszą być prowadzone w języku polskim. Wszystkie dokumenty muszą być przygotowane w polskiej wersji językowej, z wyjątkiem dokumentacji do wdrażanych produktów, która może być dostarczona w języku angielskim.
- T68.** System musi posiadać interfejs w języku polskim, dopuszcza się aby konsole tylko dla Administratorów Systemu (do jego konfiguracji) były w angielskiej lub polskiej wersji językowej.
- T69.** System powinien być zaprojektowany w sposób umożliwiający jak najszerszy zakres parametryzacji systemu przez Zamawiającego (np. konfiguracja powiadomień, modyfikacja ról systemowych, modyfikacja słowników).
- T70.** System powinien zarządzać uprawnieniami w oparciu o role, które definiować będzie mógł Administrator Systemu.
- T71.** Role użytkowników muszą być w pełni konfigurowalne w zakresie definiowania zakresu uprawnień.

- T72.** System musi pobierać informacje o użytkowniku jak i o grupie z Active Directory.
- T73.** Cała dokumentacja musi być przygotowana w postaci dokumentów MS Word (format .docx)
- T74.** Wykonawca dostarczy architekturę systemu w formie pliku Microsoft Visio (plik w formacie *.vsdx) zawierającą wszystkie komponenty serwerowe, z parametrami technicznymi serwerów, nazwami, adresami oraz połączeniami pomiędzy komponentami z wskazaniem kierunku połączenia, portów tcp/udp oraz wymaganych protokołów.
- T75.** Rozwiązanie musi posiadać czytelny plik z logami.
- T76.** Rozwiązanie musi umożliwiać integrację z systemami bezpieczeństwa typu SIEM w zakresie przesyłania logów do rozwiązania SIEM min. za pomocą mechanizmu Syslog. Wspierana musi być komunikacja Syslog szyfrowana za pomocą TLS. Dopuszczalne jest rozwiązanie, w którym System generuje logi w standardowym formacie tekstowym (zawierającym m.in. sygnatury zgodne z Syslog), natomiast ich transmisja do systemu SIEM realizowana jest poprzez dedykowanego agenta lub usługę forwardującą (np. rsyslog, syslog-ng, nxlog lub agent SIEM Zamawiającego), która umożliwia wysyłkę Syslog również w trybie TLS.
- T77.** System należy zbudować w oparciu o jeden standard serwerowych systemów operacyjnych tj. stosowane powinny być tylko serwery MS Windows Server lub Red Hat Enterprise Linux, jednocześnie dopuszczalny jest wyjątek dla serwerów baz danych.
- T78.** Instalatory dla komponentów serwerowych należy dostarczyć w natywnym dla danego systemu operacyjnego formacie tj. RPM dla Red Hat Enterprise Linux lub MSI/EXE dla Windows Server.
- T79.** Parametry dla aplikacji WEB wysyłane muszą być metodą POST, nie dopuszcza się przesyłania parametrów za pomocą metody GET.
- T80.** Wykonawca w pierwszej kolejności dostarczy procedury instalacyjne dla środowiska TST. System PRD powinien zostać zainstalowany po uruchomieniu i rozwiązaniu ewentualnych problemów na środowisku TST.
- T81.** Połączenie z bazą danych: System (serwery aplikacyjne) muszą automatycznie połączyć się z bazą danych w przypadku utraty połączenia wynikającego z awarii sieci lub jednego z serwerów bazodanowych w klastrze. Zastosowane metody i sterowniki do połączenia z bazą danych muszą być odporne na krótkotrwałą utratę połączenia.
- T82.** Monitoring techniczny: System i poszczególne jego komponenty (serwery) musi umożliwiać monitorowanie obciążenia, wydajności poszczególnych komponentów i jego zasobów oraz dostarczać mechanizmy automatycznych ostrzeżeń o zagrożeniach dotyczących jego funkcjonowania do zewnętrznego systemu technicznego monitorowania (system monitorowania nie jest objęty zakresem Projektu). System technicznego monitorowania stosowany u Zamawiającego to Vmware vRealize Operations.
- T83.** Dostarczone produkty i oprogramowanie nie mogą być na liście produktów, dla których wsparcie Producenta zostanie zakończone w ciągu 42 miesięcy od dnia złożenia oferty.

WYMAGANIA BEZPIECZEŃSTWA

I. WYMAGANIA PODSTAWOWE

1.1. Uwierzytelnianie i kontrola dostępu użytkownika

- 1.1.1. Standardowy użytkownik Systemu musi być uwierzytelniany według ustalonych w PSG metod. Zalecana metoda autentykacji to mechanizm jednorazowego uwierzytelnienia (Single Sign-On) powiązany z kontem użytkownika w domenie Active Directory PSG.
- 1.1.2. Każdy użytkownik Systemu musi posiadać indywidualne konto, pozwalające na jego jednoznaczną identyfikację.
- 1.1.3. System musi zawierać możliwość tworzenia lokalnych kont dla użytkowników pełniących funkcję administratorów IT.
- 1.1.4. Podczas tworzenia haseł dla Systemu musi żądać stosowania się do wymagań wynikających z przyjętego w PSG dokumentu „Zasady Bezpieczeństwa Teleinformatycznego w PSG sp. z o.o.”. System musi mieć określoną politykę haseł tak, aby tworzone hasła nie były proste do złamania (określona minimalna długość, konieczność stosowania znaków specjalnych, małych i dużych liter, okresowa zmiana itp.).
- 1.1.5. Wymaga się, aby skrót hasła przechowywany w Systemie był wyliczany za pomocą bezpiecznej do zastosowań kryptograficznych funkcji mieszającej z wykorzystaniem tzw. mechanizmu soli (ang. Hashing with Salt). Wymagane jest stosowanie min. 32-bajtowej, losowej soli, innej dla każdego hasła. Nie dopuszcza się używania tej samej soli dla różnych i kolejnych haseł. Wymagane jest stosowanie jednej z następujących funkcji hashujących: BCrypt lub SCrypt. Dopuszcza się stosowanie funkcji hashującej SHA-2 pod warunkiem akceptacji przez Zamawiającego ilości iteracji wielokrotnego hashowania (minimum 5000 iteracji). Nie dopuszcza się przechowywania w bazach danych, czy w innych częściach Systemu haseł zapisanych otwartym tekstem.
- 1.1.6. System musi posiadać możliwość raportowania i automatycznego monitorowania i logowania aktywności użytkowników., w szczególności: udanych i nieudanych prób logowania Użytkowników, zmiany haseł etc.
- 1.1.7. Systemy operacyjne i bazy danych
 - a) muszą posiadać włączone mechanizmy śledzenia zdarzeń i rozliczalności pozwalające jednoznacznie zidentyfikować Użytkownika lub proces,

który wykonał określone działania lub zmiany w Systemie.

b) muszą zapewniać funkcjonalność rejestrowania wszystkich istotnych z punktu widzenia bezpieczeństwa zdarzeń w Systemie informatycznym, w szczególności: udanych i nieudanych prób logowania Użytkowników, zmiany haseł etc.

- 1.1.8. Wszystkie rozpoczęte przez użytkowników Systemu sesje, po określonym w konfiguracji czasie bezczynności, muszą automatycznie blokować dostęp do Systemu. Funkcjonalność ta realizowana jest przez polityki Active Directory PSG. W przypadku, kiedy konto użytkownika w Systemie nie jest powiązane z AD, funkcjonalność blokowania sesji po określonym czasie bezczynności musi być realizowana przez System. W uzasadnionych przypadkach można zrezygnować z blokowania sesji użytkownikom – za zgodą Kierownika Biura Bezpieczeństwa Teleinformatycznego i Kierownika Biura Infrastruktury Teleinformatycznej w Departamencie Teleinformatyki.

1.2. Zarządzanie uprawnieniami

- 1.2.1. System musi udostępniać mechanizm wielopoziomowego hierarchizowania uprawnień do jego zasobów z możliwością przydzielania i odbierania uprawnień przez administratora Systemu lub domeny Active Directory PSG.
- 1.2.2. W Systemie musi być uwzględniona zasada przyznawania użytkownikom minimalnych uprawnień, niezbędnych do wykonywania obowiązków służbowych.
- 1.2.3. Zaleca się, aby w Systemie zostały zaprojektowane role wraz ze wskazaniem ich zakresu zadań i odpowiedzialności.
- 1.2.4. W eksploatowanym Systemie nie dopuszcza się istnienia aktywnych, standardowych, domyślnych kont użytkownika. Niezwłocznie po zakończeniu instalacji Systemu, takie konta muszą zostać wyłączone.
- 1.2.5. Wykonawca musi szczegółowo określić niezbędne do działania Systemu wymagania w zakresie infrastruktury sieciowej i systemowej stosując zasadę przyznawania minimalnych, potrzebnych do poprawnej pracy uprawnień (np. wymagania w zakresie komunikacji sieciowej z dokładnością do portów TCP/UPD, uprawnienia do usług katalogowych Active Directory PSG).

1.3. Aplikacje klienckie

- 1.3.1. Aplikacje klienckie muszą pracować poprawnie na systemie operacyjnym w jego aktualnie wspieranej wersji.

- 1.3.2. Aplikacje klienckie muszą pracować poprawnie w kontekście standardowego użytkownika systemu operacyjnego.
- 1.3.3. Aplikacje klienckie na stacjach roboczych muszą umożliwiać pracę z Systemem dopiero po właściwym uwierzytelnieniu użytkownika (może być zintegrowane z mechanizmami systemowymi, domenowymi itp.).
- 1.3.4. Jeśli System przewiduje pracę terminalową, to aplikacja kliencka musi prawidłowo działać na eksploatowanych w PSG serwerach terminalowych.

1.4. Zabezpieczenia transmisji danych

- 1.4.1. Zabezpieczenia, które są dopuszczone do stosowania w Systemie i połączeniach do niego muszą uwzględniać wersje protokołów, które w momencie projektowania lub rozbudowy Systemu są powszechnie uznawane za bezpieczne.
- 1.4.2. System musi umożliwiać szyfrowanie informacji przesyłanych przez sieci LAN/WAN/Internet, co gwarantuje ich poufność i integralność.
- 1.4.3. PSG wymaga stosowania kryptograficznej ochrony informacji dla całej komunikacji sieciowej.
- 1.4.4. Zalecany sposób transmisji danych do przeglądarki WWW jest szyfrowanie przepływu danych poufnych, w szczególności należy wykorzystać szyfrowanie danych protokołem TLS (w jego bezpiecznej wersji) podczas komunikacji przy pomocy przeglądarki. System musi być wyposażony w certyfikaty SSL (w jego bezpiecznej wersji) dla serwerów WWW, a transmisja danych poufnych musi odbywać się z wykorzystaniem do tego celu protokołu HTTPS.

1.5. Optymalizacja pracy Systemu

- 1.5.1. Konfiguracje wszystkich serwerów muszą podlegać procesowi optymalizacji działania i poprawy stanu zabezpieczeń (hardeningu) na podstawie zaleceń producentów wykorzystywanego oprogramowania oraz ogólnie uznanych za poprawne i standardów bezpieczeństwa. W szczególności hardening musi obejmować:
 - a) instalację wyłącznie niezbędnych pakietów oprogramowania (lub usunięcie zbędnych),
 - b) określenie polityki haseł i polityki blokowania kont użytkowników,
 - c) instalację i uruchamianie wyłącznie niezbędnych usług sieciowych (lub wyłączenie zbędnych),
 - d) ustalenie restrykcyjnych praw dostępu do wszystkich krytycznych obiektów w Systemie,

- e) aktualizację wszystkich komponentów wdrażanego Systemu do najnowszej wersji oraz zapewnienie takiej aktualizacji po oddaniu Systemu do użytkowania,
 - f) opublikowanie usługi przez Web Application Firewall stosowany w PSG,
 - g) parametry udostępnionych usług sieciowych.
- 1.5.2. Serwery dedykowane dla Systemu nie mogą udostępniać innych usług i zasobów, które nie są zgodne z ich przeznaczeniem.

1.6. Zapewnienie ciągłości działania Systemu

- 1.6.1. W celu zapewnienia odpowiedniego poziomu niezawodności oraz wydajności serwerów, muszą być stosowane rozwiązania sprzętowe i programowe, zapewniające dostępność przetwarzanych w tym Systemie informacji (np. macierze dyskowe, klastry).
- 1.6.2. Zaleca się utworzenie dla Systemu środowiska testowego i środowiska deweloperskiego.
- 1.6.3. Zaleca się przeprowadzenie testów wydajnościowych Systemu przed oddaniem go do użytkowania.
- 1.6.4. System musi być objęty archiwizacją danych. Zaleca się wykonywanie kopii zapasowej: Systemu, zainstalowanego oprogramowania użytkowego oraz przetwarzanych danych zgodnie z przyjętą w tym zakresie w PSG polityką backupu. System musi też zapewniać możliwość wykonywania kopii bezpieczeństwa (backup) danych należących do programów systemowych i aplikacji produkcyjnych.
- 1.6.5. Systemy operacyjne oraz aplikacje produkcyjne Systemu muszą umożliwiać instalację poprawek, w szczególności tych dotyczących bezpieczeństwa.
- 1.6.6. Oprogramowanie antywirusowe, powinno być zainstalowane na wszystkich serwerach Systemu.
- 1.6.7. Stosowane w Systemie rozwiązania nie mogą uniemożliwiać aktualizacji sygnatur programów antywirusowych.

1.7. Rejestrowanie zdarzeń systemowych

- 1.7.1. Systemy operacyjne i bazy danych Systemu muszą posiadać mechanizmy śledzenia zdarzeń i rozliczalności (audyt i accounting) pozwalające jednoznacznie zidentyfikować użytkownika lub proces, który wykonał określone działania lub zmiany w Systemie.
- 1.7.2. Systemy operacyjne serwerów jak i bazy danych muszą zapewniać funkcjonalność rejestrowania wszystkich istotnych z punktu widzenia bezpieczeństwa zdarzeń, w szczególności: udanych i nieudanych prób logowania użytkowników, zmiany haseł etc.
- 1.7.3. System musi umożliwiać przechowywanie i zarządzanie zdarzeniami (logi) oraz ich eksport zgodnie z ustaloną na etapie realizacji procedurą przechowywania.

- 1.7.4. Mechanizmy śledzenia zdarzeń i rozliczalności oraz informacje w dziennikach zdarzeń (logi) muszą być chronione przed manipulacją i nieuprawnionym dostępem.
- 1.7.5. Do dzienników zdarzeń lub ich archiwów, mogą mieć dostęp wyłącznie osoby uprawnione. System musi zapewniać integralność dzienników zdarzeń.
- 1.7.6. System musi zapewniać synchronizację czasu ze wskazanym w tym zakresie wzorcowym źródłem czasu w PSG.

1.8. Testy bezpieczeństwa

- 1.8.1. Wykonawca Systemu musi przedstawić w Planie Wdrożenia Systemu koncepcję realizacji testów bezpieczeństwa w kontekście realizowanego projektu.
- 1.8.2. Testy wykonane zostaną przez Wykonawcę w oparciu o wcześniej uzgodniony i zaakceptowany przez Zamawiającego Plan testów bezpieczeństwa.
- 1.8.3. Plan testów bezpieczeństwa zostanie opracowany przez Wykonawcę. Wykonawca musi uzyskać akceptację Planu testów bezpieczeństwa przez Zamawiającego na minimum 30 dni przed rozpoczęciem testów.
- 1.8.4. Plan testów bezpieczeństwa musi obejmować co najmniej:
 - a) opracowanie scenariuszy testowych (utworzenie do nich kroków testowych z wartościami oczekiwanymi),
 - b) określenie warunków początkowych niezbędnych do wykonania każdego scenariusza testowego oraz sposobu wykonania każdego scenariusza testowego,
 - c) wykonanie scenariuszy testowych,
 - d) rejestrację i zgłoszenie do PSG defektów powodujących negatywny wynik określonych scenariuszy testowych,
 - e) wykonanie poprawek do zgłoszonych defektów,
 - f) harmonogram testów,
 - g) przypisanie zasobów ludzkich po stronie PSG (wraz z terminami) niezbędnych do realizacji testów,
 - h) wymagania infrastruktury niezbędne do realizacji testów.
- 1.8.5. PSG zastrzega sobie prawo do uczestnictwa w realizowanych przez Wykonawcę testach bezpieczeństwa oraz do samodzielnego przeprowadzenia testów bezpieczeństwa przy współpracy z Wykonawcą.

- 1.8.6. PSG zastrzega sobie prawo do przeprowadzenia pentestów bezpieczeństwa we własnym zakresie lub przez stronę trzecią – na koszt Zamawiającego. W przypadku dostępu Zamawiającego do kodów źródłowych Systemu, Zamawiający zastrzega sobie prawo do przeprowadzenia testów bezpieczeństwa kodu źródłowego przez stronę trzecią.
- 1.8.7. Wykonawca Systemu wytworzy dokumentację (raport z wykonanych testów) uwzględniającą wykonywane czynności oraz wyniki działań w ramach testów bezpieczeństwa.
- 1.8.8. Wykonawca Systemu uwzględni zalecenia i uwagi wynikające z testów bezpieczeństwa, następnie przeprowadzi kolejne testy bezpieczeństwa, po których Wykonawca wytworzy raport końcowy.

II. WYMAGANIA DLA USŁUG IT UDOSTĘPNIANYCH PRZEZ PRZEGLĄDARKĘ

System musi być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project).

1. Serwis hostowany na systemie operacyjnym (OS) w aktualnej wersji: Windows Server 2022 lub nowszy.
2. Aktualizacje systemów operacyjnych (OS), komponentów OS, baz danych, Content Management System (CMS) i innych komponentów wykorzystywanych w CMS wykonywane minimum raz w miesiącu.
3. Zabezpieczenie serwisu za pomocą Web Application Firewall (WAF) PSG.
4. Odporność na wszystkie rodzaje ataków typu Injection, w tym Code Injection, SQL Injection, XML Injection, itp.
5. Obsługa tylko najnowszych protokołów szyfrowania ruchu tj. TLS 1.3 lub 1.2 oraz algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Wykonawca przeprowadzał będzie weryfikację konfiguracji SSL minimum raz w miesiącu i w razie potrzeby utwardzał konfigurację, tak aby serwis został oceniony na A+ za pomocą narzędzia dostępnego pod adresem: <https://www.ssllabs.com/ssltest/>. Nie mogą być stosowane żadne protokoły i algorytmy wskazane w serwisie <https://www.ssllabs.com/ssltest/> jako słabe (weak) lub niebezpieczne (insecure). Wymagane jest zapewnienie obsługi protokołu TLS 1.3 zgodnego z RFC 8446.
6. Baza danych serwisu umieszczona na dedykowanym serwerze lub serwerach, oddzielnym (oddzielnym) od serwerów aplikacyjnych. Baza danych musi znajdować się na serwerze, który nie będzie świadczył innych usług.

7. Wykonawca zapewni Hardening (utwardzanie) systemów operacyjnych serwerów aplikacyjnych i bazodanowych zgodnie z wymaganiami CIS Benchmark dla stosowanego OS. Jeżeli dostępne będą Benchmarki CIS dla stosowanego rozwiązania (np. bazy danych i serwera WEB) Wykonawca zapewni hardening dla tych komponentów zgodnie z określonymi tam wytycznymi.
8. Musi być Wykorzystywany dostarczony przez Zamawiającego (PSG), komercyjny certyfikat SSL.
9. Serwis musi poprawnie działać w następujących przeglądarkach w ich aktualnej wersji:
- dla aplikacji wewnętrznych (tylko dla pracowników PSG):
 - a) w systemie Windows w jego aktualnie wspieranej wersji: Microsoft Edge,
 - b) w systemie macOS: Microsoft Edge, Safari,
 - c) w systemie iOS: Safari,
 - d) w systemie Android: Google Chrome, Mozilla Firefox.
 - dla aplikacji zewnętrznych (dla Klientów PSG):
 - a) w systemie Windows w jego aktualnie wspieranej wersji: Microsoft Edge, Google Chrome, Opera, Safari, Mozilla Firefox,
 - b) w systemie macOS: Microsoft Edge, Safari, Google Chrome, Opera, Mozilla Firefox,
 - c) w systemie iOS: Google Chrome, Safari,
 - d) w systemie Android: Google Chrome, Mozilla Firefox.
10. Serwis musi być dostarczony równolegle w wersji optymalizowanej dla przeglądarek na Urządzenia typu desktop (Windows w jego aktualnie wspieranej wersji, macOS, Linux) oraz w wersji optymalizowanej dla Smartphone z iOS i Android. Serwis musi automatycznie wykrywać typ przeglądarki i dopasowywać wygląd serwisu.
11. W przypadku, jeśli dostęp będzie wymagany dla personelu podmiotów zewnętrznych musi odbywać się za pomocą połączenia VPN z siecią PSG i poprzez terminal przesiadkowy JumpHost.
12. Stosowanie wymuszania HTTPS oraz przekierowania z HTTP na HTTPS, nagłówek wymuszający HTTPS (nagłówek Strict-Transport-Security).
13. Serwis dostarczany domyślnie za pomocą protokołu HTTP/2, zachowany tryb zgodności wstecznej z HTTP/1.1 wyłącznie dla starszych przeglądarek (tj. nie obsługujących HTTP/2 lub nowszego).
14. Stosowanie restrykcyjnych nagłówków HTTP zwiększających bezpieczeństwo aplikacji webowej, w tym minimum: Content-Security-Policy, Expect-CT (wartość enforce, max-age=30), X-Content-Type-Options (wartość nosniff), X-XSS-Protection (wartość 1; mode=block), Referrer-Policy, Strict-Transport-Security, X-Frame-Options, Feature-Policy
15. Nagłówek Content-Security-Policy musi być skonfigurowany w sposób restrykcyjny, nie jest dopuszczalne stosowanie dyrektywy 'unsafe-eval' dla skryptów.
16. Automatyczny bufor cache dla statycznych zawartości.

17. Ustawianie mime-type dla każdej zawartości zwracanej przez serwis.
18. W nagłówkach, komunikatach błędów oraz odpowiedziach z serwisu ukrywanie zastosowanych technologii oraz wersji komponentów, wersji systemów operacyjnych, wersji używanych silników, wersji CSM (np. zwracany nagłówek http Server o wartości „PSG”).
19. Grafiki zamieszczane w serwisie w optymalnym formacie dopasowanym do nowoczesnych przeglądarek oraz w starszych formatach dla starszych przeglądarek tj. w formacie WebP dla nowoczesnych przeglądarek oraz w formatach jpg, png, gif dla przeglądarek nieobsługujących formatu WebP.

III. ZALECENIA STANDARDU OWASP TESTING GUIDE

System musi spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0.2 co najmniej na poziomie pierwszym (L1), w tym obligatoryjnie wymagania wyszczególnione poniżej.

1. Wymagania weryfikacji dla architektury, projektowania i modelowania zagrożeń

Wszystkie komponenty aplikacji są zidentyfikowane, znane i rzeczywiście potrzebne.

2. Wymagania weryfikacji dla uwierzytelniania

- 2.1. Wszystkie strony oraz zasoby standardowo wymagają uwierzytelnienia, za wyjątkiem tych, które mają być dostępne publicznie (zasada pełnej mediacji).
- 2.2. Pola zawierające dane uwierzytelniające nie są uzupełniane przez aplikację. Propozycje uzupełniania realizowane przez aplikację oznacza, że są one przechowywane czystym tekstem lub w odwracalnym formacie, co jest zabronione.
- 2.3. Wszystkie mechanizmy uwierzytelniania są wymuszane po stronie serwera.
- 2.4. Wszystkie mechanizmy uwierzytelniania, które kończą pracę niepowodzeniem, robią to w sposób bezpieczny, aby mieć pewność, że atakujący nie może się zalogować.
- 2.5. Pole dla hasła zezwala lub sprzyja używaniu haseł (passphrase) i nie ma wprowadzonych ograniczeń chroniących przed korzystaniem z menedżerów haseł oraz wpisywaniem długich lub bardzo złożonych haseł.
- 2.6. Wszystkie operacje dotyczące uwierzytelniania (takie jak rejestracja, aktualizacja profilu, przypomnienie loginu, przypomnienie hasła, unieważnienie zgubionego kodu do telefonicznej obsługi klienta lub automatycznej obsługi klienta), które powodują odzyskanie dostępu do konta, posiadają przynajmniej takie same zabezpieczenia jak podstawowe mechanizmy uwierzytelniania.
- 2.7. Funkcja zmiany hasła zawiera konieczność podania hasła obecnie używanego, nowego hasła oraz konieczność ponownego wpisania nowego hasła.
- 2.8. Dane uwierzytelniające są przesyłane wykorzystując właściwy zaszyfrowany link oraz wszystkie strony/funkcje, które wymagają by użytkownik podał dane uwierzytelniające wymagają takiego szyfrowanego linku.

- 2.9. Mechanizmy odzyskiwania hasła nie ujawniają dotychczasowych hasel i nowe hasło nie jest przesyłane w formie jawnej do użytkownika.
- 2.10. Nie jest możliwa enumeracja wykorzystująca loginy użytkowników, funkcję resetowania hasła lub funkcjonalność przypomnienia nazwy użytkownika.
- 2.11. Platforma lub inne komponenty, z których korzysta aplikacja nie używają domyślnych hasel (np. admin/password).
- 2.12. Wdrożono mechanizmy przeciwdziałające automatyzacji, aby zapobiegać testowaniu ujawnionych danych uwierzytelniających, atakom brute force i atakom blokującym konta.
- 2.13. Funkcje odzyskiwania hasła i inne ścieżki odzyskiwania poświadczeń uwzględniają użycie tokenu udostępniającego jednorazowe, zmienne w czasie hasła (Timebased One-Time Password algorithm - TOTP) lub innego tokena programowego, mechanizmu push lub mechanizmu odzyskiwania offline. Wykorzystywanie losowych wartości przesyłanych pocztą elektroniczną lub SMS powinno być jedynie ostatecznością, gdyż dowiedziono ich słabości.
- 2.14. Wykorzystywane współdzielone sekretne pytania, nie naruszają przepisów dotyczących prywatności i są na tyle trudne by w rzeczywistości chronić aplikację.
- 2.15. Wdrożono mechanizmy blokujące użycie znanych lub słabych hasel.
- 2.16. Aplikacja pozwala użytkownikom na uwierzytelnienie przy wykorzystaniu uprawnionego bezpiecznego mechanizmu uwierzytelniania.
- 2.17. Interfejs administracyjny nie jest dostępny dla stron niezaufanych.
- 2.18. Funkcja autouzupełniania w przeglądarce lub integracja z menedżerami hasel muszą być dopuszczone, chyba że są zabronione na podstawie przeprowadzonej analizy ryzyka.

3. Wymagania weryfikacji dla zarządzania sesją

- 3.1. Aplikacja nie używa zmodyfikowanego managera sesji lub, jeśli jest on używany, to jest odporny na wszystkie powszechne ataki na zarządzanie sesją.
- 3.2. Sesje są unieważniane po wylogowaniu się użytkownika.
- 3.3. Sesje wygasają po określonym czasie bezczynności.
- 3.4. Wszystkie strony, do których dostęp wymaga uwierzytelnienia, zawierają łatwy i widoczny dostęp do funkcji wylogowania.
- 3.5. Identyfikatory sesji nigdy nie są ujawniane w URL, w komunikatach błędów lub logach. Należy również zweryfikować, czy aplikacja nie wspiera przepisywania w URL ciasteczek sesyjnych (ang. URL-rewriting).
- 3.6. Każde pomyślne uwierzytelnienie, a także ponowne uwierzytelnienie, tworzy nową sesję z nowym identyfikatorem.
- 3.7. Identyfikatory sesji przechowywane w ciasteczkach mają ustawioną ścieżkę z wartością odpowiednio restrykcyjną dla danej aplikacji i tokeny sesji uwierzytelniania mają dodatkowo ustawione atrybuty "HttpOnly" i "secure".
- 3.8. Aplikacja ogranicza liczbę jednoczesnych aktywnych sesji.
- 3.9. Lista aktywnych sesji jest wyświetlana dla każdego użytkownika w profilu konta lub podobnym. Użytkownik musi posiadać możliwość zakończenia dowolnej aktywnej sesji.

3.10. Użytkownik ma zaproponowaną opcję zakończenia wszystkich innych aktywnych sesji, po pomyślnym zakończeniu procesu zmiany hasła.

4. Wymagania weryfikacji dla kontroli dostępu

- 4.1. Została wdrożona zasada minimalnych uprawnień - użytkownicy powinni mieć dostęp tylko do funkcji, plików, linków URL, usług oraz innych zasobów, do których posiadają zezwolenie.
- 4.2. Dostęp do wrażliwych zapisów jest chroniony w taki sposób, aby tylko autoryzowane obiekty lub dane były dostępne dla użytkownika.
- 4.3. Listowanie katalogów jest wyłączone. Dodatkowo aplikacje nie mogą pozwalać na odkrycie lub ujawnienie plików lub metadanych katalogów takich jak Thumbs.db, .DS_Store, .git lub foldery .svn.
- 4.4. Mechanizmy kontroli dostępu, które kończą pracę niepowodzeniem, robią to w sposób bezpieczny.
- 4.5. Te same reguły kontroli dostępu występujące w warstwie prezentacji są również egzekwowane po stronie serwera.
- 4.6. Aplikacja bądź platforma generuje silne, losowe tokeny zabezpieczające przed atakami typu CSRF lub posiada inne mechanizmy ochrony transakcji.
- 4.7. Aplikacja w poprawny sposób wymusza autoryzację zależną od kontekstu, tak aby nie umożliwiać nieautoryzowanych manipulacji realizowanych poprzez zmiany wartości parametrów.

5. Wymagania weryfikacji dla obsługi złośliwych danych wejściowych

- 5.1. Środowisko uruchomieniowe nie jest podatne na przepełnienia bufora lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu przepełnienia bufora.
- 5.2. Wszystkie prowadzone po stronie serwera walidacje wejścia, które zakończone są niepowodzeniem, powodują odrzucenie żądania oraz są logowane.
- 5.3. Wszystkie mechanizmy walidacji są egzekwowane po stronie serwera.
- 5.4. Wszystkie kwerendy SQL, HQL, OSQL, NOSQL, składowane procedury, wywołania składowanych procedur są chronione poprzez wykorzystywanie przygotowanych zapytań lub sparametryzowanych kwerend, i tym samym nie są podatne na atak SQL Injection.
- 5.5. Aplikacja nie jest podatna na atak LDAP Injection lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takiego ataku.
- 5.6. Środowisko uruchomieniowe nie jest podatne na atak wstrzyknięcia komend systemu operacyjnego lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takiego ataku.
- 5.7. Aplikacja nie jest podatna na ataki zdalnego lub lokalnego dołączenia plików (Remote File Inclusion - RFI lub Local File Inclusion - LFI) gdy wykorzystywana jest treść będąca ścieżką do plików.
- 5.8. Aplikacja nie jest podatna na ataki XML Injection, XML External Entity, XPath query lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takich ataków.
- 5.9. Wszystkie łańcuchy zmiennych włączane w HTML lub inny kod uruchamiany po stronie klienta webowego są albo w poprawny sposób ręcznie wprowadzone

w sposób zależny od kontekstu, albo wykorzystują szablony, wprowadzając je automatycznie w sposób zależny od kontekstu, aby zapewnić, że aplikacja nie jest podatna na ataki XSS typu „reflected”, „stored” i DOM.

5.10. Niezaufany kod HTML z edytorów WYSIWYG lub podobnych jest wyczyszczony oraz obsługiwany odpowiednio w zakresie walidacji wejścia i enkodowania wyjścia.

6. Wymagania weryfikacji dla nieaktywnych mechanizmów kryptograficznych

6.1. Wszystkie moduły kryptograficzne, które kończą pracę niepowodzeniem robią to w sposób bezpieczny, a błędy są obsługiwane w sposób zapobiegający atakom oracle padding.

6.2. Wszystkie moduły kryptograficzne wykorzystywane przez aplikację zostały sprawdzone na zgodność ze standardem FISP 140-2 lub równorzędnym.

7. Wymagania weryfikacji dla obsługi i logowania błędów

7.1. Aplikacja nie zwraca komunikatów o błędach lub śladów stosu (stack traces), które zawierają dane wrażliwe i które mogą pomóc atakującym. Zawierają się w tym identyfikatory sesji, wersje oprogramowania/platformy i dane osobowe.

7.2. Źródła czasu są synchronizowane, aby zapewnić, że logi mają poprawny czas.

8. Wymagania weryfikacji dla mechanizmów ochrony danych

8.1. Dla wszystkich formularzy zawierających dane wrażliwe, wyłączone jest cachowanie po stronie klienta, włączając w to funkcjonalność automatycznego wypełnienia pól.

8.2. Wszystkie dane wrażliwe są przesyłane do serwera wewnątrz wiadomości HTTP lub jej nagłówka (np. parametry URL nie muszą być używane do przesyłania danych wrażliwych).

8.3. Aplikacja posiada ustawienia w nagłówku, uniemożliwiające cachowanie danych odpowiednie do założonego ryzyka aplikacji.

8.4. Dane przechowywane po stronie klienta (takie jak lokalnie przechowywane informacje o sesjach HTML5, przechowywane sesje, IndexedDB, ciasteczka: zwykle i Flash), nie zawierają danych podlegających ochronie oraz danych osobowych.

9. Wymagania weryfikacji dla zabezpieczania komunikacji

9.1. Możliwe jest zbudowanie ścieżki od zaufanego CA do każdego serwerowego certyfikatu Transport Layer Security (TLS) i każdy certyfikat serwera jest ważny.

9.2. Dla wszystkich połączeń (zewnętrznych i wewnętrznych), które są uwierzytelniane lub związane z wrażliwymi danymi lub funkcjami, jest wykorzystywany TLS a także nie jest możliwe pogorszenie parametrów połączenia do połączenia niezabezpieczonego. Preferowany jest najsilniejszy dostępny algorytm szyfrowania.

9.3. Nagłówki HTTP Strict Transport Security są włączone do wszystkich zapytań i dla wszystkich poddomen np. w postaci: Strict-Transport-Security: max-age=15724800; includeSubdomains.

- 9.4. W celu zmniejszenia prawdopodobieństwa pasywnych ataków polegających na zapisywaniu ruchu, używane są szyfry wspierające doskonałe utajnienie przekazywania (forward secrecy).
- 9.5. Są włączone i właściwie skonfigurowane mechanizmy unieważniania certyfikatów, takie jak „zszywanie” odpowiedzi Online Certificate Status Protocol (OSCP).
- 9.6. Używane są tylko silne algorytmy, szyfry i protokoły w ramach całej hierarchii certyfikatów, włącznie z certyfikatem root i certyfikatami pośrednimi w ramach wybranego urzędu certyfikacji.
- 9.7. Konfiguracja TLS jest zgodna z bieżącymi najlepszymi praktykami szczególnie dlatego, że popularne ustawienia, szyfry i algorytmy z czasem mogą okazać się niebezpieczne.

10. Wymagania weryfikacji dla konfigurowania bezpieczeństwa HTTP

- 10.1. Aplikacja akceptuje tylko zdefiniowany zestaw metod zapytań HTTP, takich jak GET i POST oraz nieużywane metody (takie jak TRACE, PUT, DELETE) są w sposób wyraźny zablokowane.
- 10.2. Każda odpowiedź HTTP zawiera nagłówek „content type”, określający bezpieczny zestaw znaków (np. UTF-8, ISO 8859-1).
- 10.3. Nagłówki HTTP lub jakakolwiek część odpowiedzi HTTP nie ujawniają szczegółowej informacji o wersjach komponentów systemu.
- 10.4. Wszystkie odpowiedzi z API zawierają nagłówki X-Content-Type-Options: nosniff i ContentDisposition: attachment; filename="api.json" (lub inne nazwy plików odpowiednie dla jego typu).
- 10.5. Mechanizm Content Security Policy V2 (CSP) jest używany, aby zapobiegać podatnościom wstrzyknięcia DOM, XSS, JSON i JavaScript.
- 10.6. Nagłówek X-XSS-Protection: 1; mode=block jest użyty by uruchomić w przeglądarce filtry chroniące przed reflected XSS.

11. Wymagania weryfikacji dla plików i innych zasobów

- 11.1. Przeadresowania i przekierowania URL są dozwolone jedynie dla predefiniowanych (white label) stron internetowych i pokazują użytkownikowi ostrzeżenie w sytuacji przekierowania do potencjalnie niezauważanych treści.
- 11.2. Niezauważane dane z plików wysłanych do aplikacji nie są bezpośrednio przekazywane do komend wykonujących operacje na drzewie plików, w szczególności by zapewnić ochronę przed podatnościami typu „Path Traversal”, „Local File Inclusion” i „OS command injection”.
- 11.3. Pliki pozyskane z niezauważanych źródeł są walidowane pod kątem oczekiwanego typu pliku i są skanowane programem antywirusowym w celu ochrony przed szkodliwą zawartością.
- 11.4. Niezauważane dane nie są użyte bezpośrednio w mechanizmach ładowania, ładowania klas i zwracania, by zapewnić ochronę przed atakami typu „Remote/Local File Inclusion”.

11.5. Niezaufane dane nie są wykorzystywane w ramach mechanizmu „Cross-Origin Resource Sharing” (CORS), w celu zapewnienia ochrony przed potencjalnie złośliwymi zewnętrznymi treściami.

11.6. Kod aplikacji nie wykonuje danych otrzymanych z niezaufanych źródeł.

11.7. Aplikacja nie używa Flasha, Active-X, Silverlighta, NACL, appletów Java ani innej technologii klienckiej, która nie jest natywnie wspierana przez standardy W3C w przeglądarkach.

12. Wymagania weryfikacyjne dla web serwisów

12.1. Ten sam styl kodowania znaków jest wykorzystywany przez klienta i serwer.

12.2. Dostęp do funkcji administracyjnych i zarządczych w ramach aplikacji jest ograniczony do wąskiej grupy administratorów.

12.3. Schemat XML lub JSON jest stosowany i jest weryfikowany przed zaakceptowaniem danych wejściowych.

12.4. Wszystkie dane wejściowe mają odpowiednie ograniczenia długości.

12.5. Usługi sieciowe oparte o SOAP są zgodne co najmniej z profilem podstawowym Web Services Interoperability (WS-I Basic Profile). W szczególności dotyczy to szyfrowania TLS.

12.6. Uwierzytelnienie i autoryzacja dotycząca sesji są wykorzystywane. Należy unikać stosowania statycznych kluczy API i podobnych rozwiązań.

12.7. Usługi REST są chronione przed atakami typu Cross-Site Request Forgery wykorzystując co najmniej jeden mechanizm spośród weryfikacji ORIGIN, podwójnego wprowadzania szablonów ciasteczek (cookie pattern), CSRF nonces oraz sprawdzeń punktu odniesienia (referrer checks).

13. Wymagania weryfikacyjne dla procesu konfiguracji

13.1. Wszystkie komponenty muszą być aktualne, z właściwymi ustawieniami dotyczącymi bezpieczeństwa i wersjami. To powinno uwzględniać: usunięcie niepotrzebnych wpisów konfiguracyjnych i folderów takich jak przykładowe aplikacje, dokumentację platformy oraz domyślnych bądź przykładowych użytkowników.

IV. Wymagania w zakresie ochrony danych osobowych

1. System musi zapewniać odnotowanie:

- a. nazwa i adres podmiotu któremu przekazano dane;
- b. data udostępnienia danych;
- c. zakres udostępnianych danych;
- d. podstawa prawna udostępnienia;

2. Dla każdej osoby, której dane osobowe są przetwarzane, system musi zapewniać odnotowanie:

- a. daty pierwszego wprowadzenia danych do systemu;
- b. identyfikatora użytkownika wprowadzającego dane;
- c. rejestrację wszelkich zmian wykonanych na danych.

3. System musi umożliwiać konfigurację maksymalnego czasu przetwarzania danych osobowych.

4. System musi umożliwiać eksport danych osobowych dotyczących osoby, której dane są w systemie przetwarzane oraz informacji wynikających z art. 15 RODO w formie powszechnie i jednoznacznie zrozumiałej dla tej osoby (np. w postaci PDF).
5. System musi umożliwiać usunięcie całości danych dotyczących osoby lub ich pseudonimizację, szczególnie w zakresie danych osobowych szczególnej kategorii.
6. System musi umożliwiać odnotowanie informacji o zgodzie na przetwarzanie danych osobowych, osoby, której dane dotyczą.
7. Dane osobowe w systemie muszą być przechowywane w sposób zaszyfrowany.

OFERTA WYKONAWCY
w odrębnym załączniku

Załącznik nr 5 do Umowy

Wzór Protokołu odbioru do Umowy nr z dnia

spisany w dniu W

przez:

Zamawiającego: Polska Spółka Gazownictwa sp. z o.o. z siedzibą w Tarnowie, ul. Wojciecha Bandrowskiego 16, 33-100 Tarnów, Oddział Wsparcia w Warszawie, adres: ul. Krucza 6/14, 00-537 Warszawa wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000374001, NIP 525 24 96 411, REGON 142739519, o kapitale 10.685.630.000,00 zł, którą reprezentuje:

Wykonawcę:

_____ z siedzibą w _____, ul. _____, (____-____-____), wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy _____, _____ Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS _____, NIP _____, REGON _____, o kapitale zakładowym _____, którą reprezentuje:

Odbioru [wariantowo:] Zamówienia nr _____, Systemu wraz z Licencjami, Wdrożenia, dokonali przedstawiciele Zamawiającego i Wykonawcy w składzie:

ze strony Zamawiającego:

.....

ze strony Wykonawcy:

Niniejszym potwierdzamy dostarczenie i odbiór przez Zamawiającego: [wariantowo:] Systemu wraz z Licencjami, Wdrożenia, [Lub wariantowo w przypadku odbioru Sprzętu:] Sprzętu:

Lp.	Kod produktu	Nazwa Sprzętu	Ilość	Nr seryjny
1				
2				

Uwagi:

.....

Zamawiający**Wykonawca**

Wzór zamówienia nr:

Dane zamówienia

Nazwa firmy	Polska Spółka Gazownictwa sp. z o.o.
Odbiorca	Biuro Wsparcia Bezpośredniego
Projekt	
Status	
Data utworzenia	RRRR-MM-DD GG:MM:SS

Dane odbiorcy

Odbiorca	Biuro Wsparcia Bezpośredniego
Nazwa	Polska Spółka Gazownictwa sp. z o. o.
Ulica	Według wykazu z umowy
Miasto	Według wykazu z umowy
Telefon	Według wykazu z umowy
Kraj	Polska

Pozycje

Nazwa	Ilość	Cena	Wartość	Waluta	Obiekt kontrolingowy	Indeks materiału
Pozycja 1						
Podsumowanie*				PLN		
*wyliczono na podstawie kursów walut z dnia utworzenia zamówienia						

Wykaz lokalizacji dostaw i osób upoważnionych do odbioru dostaw

Miejscom dostaw są lokalizacje Polskiej Spółki Gazownictwa sp. z o.o., w których wykonywana będzie instalacja i serwis gwarancyjny urządzeń wielofunkcyjnych, wskazane w tabeli poniżej:

L.p.	Nazwa zakładu	Adres	Osoba upoważniona do odbioru Sprzętu	Telefon Email
1.	Białystok	ul. Gen. Stanisława Sosabowskiego 24, 15-182 Białystok		
2.	Bydgoszcz	ul. Jagiellońska 42, 85-097 Bydgoszcz		
3.	Gdańsk	ul. Wałowa 41/43, 80-858 Gdańsk		
4.	Gorzów Wielkopolski	ul. Sikorskiego 73, 66-400 Gorzów Wielkopolski		
5.	Jasło	ul. Floriańska 112, 38-200 Jasło		
6.	Kielce	ul. Loefflera 2, 25-550 Kielce		
7.	Koszalin	ul. Połczyńska 55/57, 75-808 Koszalin		
8.	Kraków	ul. Gazowa 16, 31-060 Kraków		
9.	Lublin	ul. Diamentowa 15, 20-471 Lublin		
10.	Łódź	ul. Targowa 18, 90-042 Łódź		
11.	Olsztyn	ul. Lubelska 42A, 10-409 Olsztyn		
12.	Opole	ul. Armii Krajowej 2, 45-071 Opole		
13.	Poznań	ul. Za Groblą 8, 61-860 Poznań		
14.	Szczecin	ul. Tama Pomorzańska 26, 70-952 Szczecin		
15.	Warszawa	ul. Równoległa 4a, 02-235 Warszawa		
16.	Wrocław	ul. Ziębicka 44, 50-507 Wrocław		
17.	Wałbrzych	ul. Wrocławska 2 58-309 Wałbrzych		
18.	Zgorzelec	ul. Fabryczna 1 59-900 Zgorzelec		
19.	Zabrze	ul. Mikulczycka 5, 41-800 Zabrze		
20.	Jarosław	ul. Krakowska 54, 37-500 Jarosław		
21.	Sandomierz	ul. K. K. Baczyńskiego 3, 27-600 Sandomierz		
22.	Rzeszów	ul. Wspólna 5, 35-205 Rzeszów		
23.	Tarnów	ul. Bandrowskiego 16, 33-100 Tarnów		

24.	Kalisz	ul. Majkowska 9, 62-800 Kalisz		
25.	Radom	Ul. Gazowa 11/13 26-600 Radom		
26.	Ciechanów	ul. Mleczarska 17, 06-400 Ciechanów		
27.	Krosno	ul. Łukasiewicza 89, Krosno 38-400		

Wykaz osób upoważnionych do składania zamówień.

L.p.	Imię i nazwisko	Telefon Email
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Wykaz osób przy pomocy, których będzie realizowany Przedmiot Zamówienia

Wymagania wobec osób przy pomocy, których będzie realizowany Przedmiot Zamówienia:

- a) specjalista ds. logistyki – co najmniej 1 (jedna) osoba – osoba odpowiedzialna za ustalenie, koordynację i dotrzymanie terminów dostaw. Zamawiający wymaga, aby osoba ta spełniała następujący warunek:
 - posiada doświadczenia w obsłudze przynajmniej jednej dostawy urządzeń wielofunkcyjnych/drukarek/sprzętu komputerowego do minimum 20 (dwudziestu) lokalizacji;
- b) specjalista ds. serwisu – co najmniej 2 (dwie) osoby – osoba odpowiedzialna za obsługę serwisową i gwarancyjną dostarczonego sprzętu. Zamawiający wymaga, aby każda z osób spełniała następujący warunek:
 - posiada minimum 3 lat w zakresie obsługi serwisowej i gwarancyjnej dostaw sprzętu informatycznego;
- c) technik ds. serwisu – co najmniej 5 (pięć) osób – osoba realizująca zgłoszenia serwisowe w zakresie obowiązków gwarancyjnych, w tym przeglądów konserwacyjnych w okresie trwania gwarancji. Zamawiający wymaga, aby każda z tych osób spełniała następujący warunek:
 - posiada odpowiednie kwalifikacje: certyfikat producenta oferowanych urządzeń uprawniający do wykonywania serwisu i konserwacji danych urządzeń uzyskany po ukończeniu autoryzowanego/ych szkolenia/ń.

Nie dopuszcza się, aby jedna osoba pełniła w Zespole więcej niż jedną funkcję.

Lp.	Imię i nazwisko	Pełniona funkcja	Posiadane certyfikaty (należy wskazać jeżeli dotyczy)	Doświadczenie
1				
2				
3				
4				
5				
6				
7				
8				

Karta materiałów do Urządzenia.

		Producent Urządzenia:				
		Model oferowanego Urządzenia:				
Kod Producenta - materiału	Kod Produktu	Opis *	Rodzaj **	Kolor ***	Wydajność	Czy musi wymieniać serwis ****

* - Przykładowe dane dla
kolumny Opis :

Zestaw Konserwacyjny utrwalacza, Image transfer unit, pojemnik na zużyty toner, Zespół podajnika dokumentów (ADF roller replacement KIT), zasobnik ze zszywkami, standardowej pojemności kartridż, wysokiej pojemności kartridż, ekstra wysokiej pojemności kartridż, zespół bębna (osobny dla każdego koloru), pojemnik na zużyty toner, Zespół utrwalający (grzałka), Rolka transferowa, Taśma transferowa, pojemnik na zużyty toner i inne dla danego modelu

** - Przykładowe dane dla
kolumny Rodzaj :

Toner, Bęben, Pojemnik na zużyty toner, Urządzenie utrwal, Rolka transferowa, Pas transmisyjny, Zestaw do konserwacji, Zestaw konserwacyjny ADF, zasobnik ze zszywkami i inne dla danego modelu

*** - Przykładowe dane dla
kolumny kolor :

czarny, niebieski, czerwony, żółty, cmyk

**** - Czy wymiana materiału
musi być realizowana
przez serwis (materiał
dostarcza Zamawiający)

Klauzula antykorupcyjna

1. Każda ze Stron zaświadcza, że w związku z wykonywaniem niniejszej Umowy zachowa należyta staranność i stosować się będzie do wszystkich obowiązujących Strony przepisów prawa w zakresie przeciwdziałania korupcji wydanych przez uprawnione organy w Polsce i na terenie Unii Europejskiej, zarówno bezpośrednio, jak i działając poprzez kontrolowane lub powiązane podmioty gospodarcze Stron.
2. Każda ze Stron zaświadcza, że wdrożyła procedury przeciwdziałania korupcji i konfliktowi interesów.
3. Każda ze Stron dodatkowo zaświadcza, że w związku z wykonywaniem niniejszej Umowy stosować się będzie do wszystkich obowiązujących Strony wymagań i regulacji wewnętrznych odnośnie standardów etycznego postępowania, przeciwdziałania korupcji, zgodnego z prawem rozliczania transakcji, kosztów i wydatków, konfliktu interesów, wręczania i przyjmowania upominków oraz anonimowego zgłaszania i wyjaśniania nieprawidłowości, zarówno bezpośrednio, jak i działając poprzez kontrolowane lub powiązane podmioty gospodarcze Stron.
4. Strony zapewniają, że w związku z zawarciem i realizacją niniejszej Umowy żadna ze Stron, ani żaden z ich właścicieli, udziałowców, akcjonariuszy, członków zarządu, dyrektorów, pracowników, podwykonawców, ani też żadna inna osoba działająca w ich imieniu, nie dokonywała, nie proponowała, ani nie obiecywała, że dokona, nie zaproponuje, ani też nie obieca, że dokona, ani nie upoważni do dokonania żadnej płatności lub innego przekazu stanowiącego korzyść finansową, ani też żadnej innej korzyści bezpośrednio lub pośrednio żadnemu z niżej wymienionych:
 - (i) członkowi zarządu, dyrektorowi, pracownikowi, ani agentowi Strony lub któregokolwiek kontrolowanego lub powiązanego podmiotu gospodarczego Stron,
 - (ii) funkcjonariuszowi publicznemu, rozumianemu jako osobie fizycznej pełniącej funkcję publiczną w znaczeniu nadanym temu pojęciu w systemie prawnym kraju, w którym dochodzi do realizacji niniejszej Umowy, lub w którym znajdują się zarejestrowane siedziby Stron lub któregokolwiek kontrolowanego lub powiązanego podmiotu gospodarczego Stron;
 - (iii) partii politycznej, członkowi partii politycznej, ani kandydatowi na urząd państwowy;
 - (iv) agentowi ani pośrednikowi w zamian za opłacenie kogokolwiek z wyżej wymienionych; ani też
 - (v) innej osobie lub podmiotowi – w celu uzyskania ich decyzji, wpływu lub działań mogących skutkować jakimkolwiek niezgodnym z prawem uprzywilejowaniem lub też w dowolnym innym niewłaściwym celu, jeżeli działanie takie narusza lub naruszałoby przepisy prawa w zakresie przeciwdziałania korupcji wydane przez uprawnione organy w Polsce i na terenie Unii Europejskiej, zarówno bezpośrednio, jak i działając poprzez kontrolowane lub powiązane podmioty gospodarcze Stron.
5. Strony są zobowiązane do niezwłocznego wzajemnego informowania się o każdym przypadku naruszenia postanowień niniejszej klauzuli antykorupcyjnej. Na pisemny wniosek każdej ze Stron, druga Strona niezwłocznie dostarczy informacje i udzieli odpowiedzi na uzasadnione pytania, które dotyczyć będą wykonywania niniejszej Umowy w zakresie zgodności z postanowieniami niniejszej klauzuli antykorupcyjnej.
6. Każda ze Stron zaświadcza, iż w okresie realizacji niniejszej Umowy zapewnia każdej osobie działającej w dobrej wierze możliwość zgłaszania naruszeń prawa za pośrednictwem poczty elektronicznej na adres: naduzycia@psgaz.pl lub sygnalista@psgaz.pl.
7. W przypadkach stwierdzenia podejrzenia działań korupcyjnych dokonanych w związku lub w celu wykonania niniejszej Umowy przez jakichkolwiek przedstawicieli każdej ze Stron, Strony zobowiązują się do współpracy w dobrej wierze w celu wyjaśnienia okoliczności dotyczących możliwych działań korupcyjnych.