

Zabrze, dnia 09.11.2022 r.

ZAPYTANIE OFERTOWE**w ramach zamówienia, realizowanego na podstawie**

art. 33 ust. 2 ustawy z dnia 3 kwietnia 2020 r. o szczególnych rozwiązaniach wspierających realizację programów operacyjnych, Dz.U.2022.1758 oraz art. 12 ust. 4 i 6 ustawy z dnia 12.03.2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, Dz.U.2022.583

A. ZAMAWIAJĄCY

Miasto Zabrze – Urząd Miejski w Zabrzu
ul. Powstańców Śląskich 5-7, 41-800 Zabrze

Wydział Zamawiający:

Wydział Oświaty, ul. Wolności 286, 41-800 Zabrze, pok. 310

tel.: (32) 373-35-48, e-mail: sekretariat_wo@um.zabrze.pl

Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcą:

Magdalena Błaszczynska tel.: (32) 37 33 548 e-mail: mblaszczynska@um.zabrze.pl

B. PRZEDMIOT ZAMÓWIENIA

Zaproszenie do złożenia oferty na:

Dostawę 100 laptopów do szkół podstawowych oraz ponadpodstawowych w Zabrzu w ramach projektu pn. „Wsparcie dla uczniów z Ukrainy- MIASTO ZABRZE”

C. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedsięwzięcie realizowane w ramach projektu:

„Wsparcie dla uczniów z Ukrainy- MIASTO ZABRZE” dofinansowanego ze środków w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014 - 2020 Oś priorytetowa: XI Wzmocnienie potencjału edukacyjnego Działanie 11.1. Ograniczenie przedwczesnego kończenia nauki szkolnej oraz zapewnienie równego dostępu do dobrej jakości edukacji elementarnej, kształcenia podstawowego i średniego Poddziałanie 11.1.6. Wzrost dostępności do edukacji ogólnej dla uczniów z Ukrainy- tryb nadzwyczajny.

I. Przedmiot Zamówienia:

Dostawa 100 laptopów do szkół podstawowych oraz ponadpodstawowych w Zabrzu w ramach projektu pn. „Wsparcie dla uczniów z Ukrainy- MIASTO ZABRZE” zgodnie ze specyfikacją ujętą w załączniku nr 2 „Kalkulacja ceny”.

Oferent, który powoła się na rozwiązania równoważne jest obowiązany wykazać, że zaproponowane rozwiązanie jest równoważne pod względem technicznym, jakościowym funkcjonalnym oraz wpisać informację w tym zakresie w załączniku nr 2- kalkulacja ceny w kolumnie „Opis przedmiotu równoważnego”.

II. Termin realizacji:

Dostawa musi być zrealizowana nie później niż 28 lutego 2023 r.

III. Zakres zamówienia

W ramach dostawy Wykonawca musi:

Dostarczyć przedmiot zamówienia zgodny ze specyfikacją ujętą w załączniku nr 2 „Kalkulacja ceny” do siedziby Zamawiającego: **Urząd Miejski w Zabrzu Wydział Oświaty, ul. Wolności 286, 41- 800 Zabrze, pok. 310** w godzinach pracy urzędu; tj. w dni robocze w godzinach od 7.30 do 15.30.

IV. KRYTERIA OCENY OFERT

1. Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny:

1) Cena brutto – 100%

V. WARUNKI UDZIAŁU W POSTĘPOWANIU

- 1) Wykonawca oświadcza, iż dysponuje odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia.
- 2) Wykonawca oświadcza, iż dysponuje wszystkimi niezbędnymi dokumentami niezbędnymi do prowadzenia działalności.

VI. PODSTAWY WYKLUCZENIA, O KTÓRYCH MOWA W ART. 108 UST. 1 P.Z.P.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 108 ust 1 pkt 1-6 p.z.p.
2. Z postępowania o udzielenie zamówienia wyklucza się, z zastrzeżeniem art. 110 ust. 2 p.z.p., Wykonawcę:
 - a) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
 - handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
 - o którym mowa w art. 228–230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
 - finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
 - o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
 - powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz.U. poz. 769),
 - przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,
 - o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
 - b) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 2.1.
 - c) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - d) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
 - e) jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

- f) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 p.z.p., doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

VII. DANE DOTYCZĄCE ZŁOŻENIA OFERTY

1. Ofertę należy sporządzić w formie pisemnej w języku polskim na Formularzu ofertowym lub według takiego samego schematu (załącznik nr 1 oraz załącznik nr 2 do niniejszego Zapytania Ofertowego) i złożyć Zamawiającemu w jeden z następujących sposobów:

- a) osobiście w siedzibie Zamawiającego tj. jak podano w punkcie A,
- b) za pośrednictwem poczty na adres Zamawiającego jw.
- c) za pośrednictwem bazy konkurencyjności:

<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>

W przypadku złożenia oferty zgodnie z lit. a) lub b), oferta musi być złożona w zamkniętym, nieprzejrzystym opakowaniu, na którym należy napisać:

- adres:

**Urząd Miejski w Zabrzu
Wydział Oświaty,
ul. Wolności 286, pok.310
41- 800 Zabrze,**

- nazwę zamówienia:

Dostawa 100 laptopów do szkół podstawowych oraz ponadpodstawowych w Zabrzu w ramach projektu pn. „Wsparcie dla uczniów z Ukrainy- MIASTO ZABRZE”

- nazwę i dokładny adres Wykonawcy;
 - napis o treści: „Nie otwierać przed upływem terminu składania ofert”
2. Termin składania ofert: **21.11.2022 r., godz. 09:00**
3. Oferta musi być podpisana przez osobę/y upoważnioną/e do reprezentowania Wykonawcy.
4. Termin realizacji zamówienia: nie później niż 28 lutego 2023 r.
5. Warunki płatności: płatność za zrealizowaną usługę po podpisaniu protokołu odbioru bez zastrzeżeń, w terminie 14 dni od otrzymania prawidłowo wystawionej faktury.
6. Termin związania ofertą: 30 dni, liczony od terminu składania ofert.

VIII. WYBÓR OFERTY

1. Złożone oferty muszą być zgodne z opisem zamówienia i warunkami zawartymi w punkcie – III-V. Oferty niezgodne z w/w punktami podlegają odrzuceniu.
2. Oferty złożone po terminie określonym w punkcie VII. 2. podlegają odrzuceniu.
3. Przy wyborze oferty, Zamawiający będzie się kierował kryteriami wyszczególnionymi w Zapytaniu ofertowym.
4. Cena ofertowa winna obejmować wszystkie koszty związane z realizacją zamówienia. Za cenę oferty uważać się będzie cenę brutto (łącznie z należnym podatkiem VAT).

IX. INFORMACJE DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Wymagania dotyczące realizacji zamówienia:
Od Wykonawcy oczekuje się: rzetelności w realizowaniu zlecenia.
2. Dokumentacja / przedmiot zamówienia: Nie dotyczy
3. Zamawiający wraz z zapytaniem ofertowym przekazuje: Formularz ofertowy i Kalkulację ceny.
4. W siedzibie Zamawiającego do wglądu są dokumenty: wniosek o dofinansowanie projektu.
5. Do czasu zawarcia umowy Zamawiający zastrzega sobie prawo do zakończenia postępowania na każdym etapie bez wyłonienia Wykonawcy oraz bez podania przyczyny.
6. Wykonawca może złożyć tylko jedną ofertę.

X. INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

W związku z przetwarzaniem Pani/ Pana danych osobowych informujemy- zgodnie art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 04.05.2016 r., Nr 119, s. 1, ze. zm.), zwanego dalej w skrócie „RODO”, iż:

A. ADMINISTRATOR DANYCH.

Administratorem Pani/Pana danych osobowych jest Prezydent Miasta Zabrze, którego siedziba mieści się w Urzędzie Miejskim w Zabrzu, 41-800, przy ul. Powstańców Śląskich nr 5-7.

B. KONTAKT Z ADMINISTRATOREM DANYCH.

Z Prezydentem Miasta Zabrze może się Pani/Pan skontaktować w sprawach związanych z ochroną danych osobowych, w następujący sposób:

- 1) pod adresem poczty elektronicznej: umz@um.zabrze.pl,
- 2) pod numerem telefonu: 32 373 33 00,
- 3) pisemnie na adres: Urząd Miejski w Zabrzu, 41-800, przy ul. Powstańców Śląskich nr 5-7 z dopiskiem „Ochrona danych osobowych”.

C. INSPEKTOR OCHRONY DANYCH.

Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w sprawach związanych z ochroną danych osobowych, w następujący sposób:

- 1) pod adresem poczty elektronicznej: iod@um.zabrze.pl
- 2) pod numerem telefonu: 32 373 33 00.
- 3) pisemnie na adres: Urząd Miejski w Zabrzu, 41-800, przy ul. Powstańców Śląskich nr 5-7 z dopiskiem „Inspektor ochrony danych”.

D. PODSTAWA PRAWNA I CELE PRZETWARZANIA DANYCH OSOBOWYCH.

1. Przetwarzanie Pani/Pana danych odbywa się w celu związanym z postępowaniem o udzielenie zamówienia publicznego.
2. Podstawą prawną zbierania Pani/Pana danych osobowych jest:
 - 2.1.niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit e) RODO), w szczególności na podstawie ustawy z dnia 08.03.1990 r. o samorządzie gminnym w związku z realizacją zadań ustawowych Miasta Zabrze;
 - 2.2.niezbędność przetwarzania do wykonania umowy, której Pani/Pan jest stroną, lub do podjęcia działań na Pani/Pana żądanie przed zawarciem umowy (art. 6 ust. 1 lit b) RODO);
 - 2.3.niezbędność przetwarzania do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit c) RODO); w szczególności na podstawie ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych oraz ustawy z dnia 27.08.2009 r. o finansach publicznych.

E. ODBIORCY DANYCH OSOBOWYCH.

Pani/Pana dane mogą zostać udostępnione odbiorcom będącym podmiotami przetwarzającymi, w szczególności świadczącym usługi IT na zlecenie Miasta Zabrze. Podmiotem świadczącym usługi IT w zakresie ewidencyjno- księgowym oraz elektronicznego obiegu dokumentów jest Asseco Data Systems S.A. z siedzibą w Gdyni. W niektórych przypadkach podmioty zewnętrzne świadczące usługi na zlecenie Miasta Zabrze mogą występować w roli niezależnych administratorów np. poczta polska lub inni operatorzy pocztowi, w tym firmy kurierskie.

F. OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH.

1. Pani/Pana dane osobowe będą przechowywane jedynie w okresie niezbędnym do spełnienia celu, dla którego zostały zebrane.

2. Po spełnieniu celu, dla którego Pani/Pana dane zostały zebrane, mogą one być przechowywane jedynie w celach archiwalnych, przez okres, który wyznaczony zostanie przede wszystkim na podstawie rozporządzenia Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, chyba że przepisy szczególne stanowią inaczej.

G. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ, W TYM DOSTĘPU DO DANYCH OSOBOWYCH.

Na zasadach określonych przepisami RODO, posiada Pani/Pan prawo do żądania od administratora:

- 1) dostępu do treści swoich danych osobowych,
- 2) sprostowania (poprawiania) swoich danych osobowych,
- 3) usunięcia swoich danych osobowych,
- 4) ograniczenia przetwarzania swoich danych osobowych,
- 5) przenoszenia swoich danych osobowych, o ile jest to technicznie możliwe i tylko w zakresie danych nieobowiązkowych, a ponadto, posiada Pani/Pan prawo do wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych.

Nie wszystkie Pani/Pana żądania będziemy jednak mogli zawsze spełnić. Zakres przysługujących praw zależy bowiem zarówno od przesłanek prawnych uprawniających do przetwarzania danych, jak i często – sposobów ich gromadzenia. Ponieważ Pani/Pana dane osobowe w Urzędzie Miasta Zabrze przetwarzane są wyłącznie w granicach wskazanych przepisami prawa, w większości przypadków nie będziemy mogli zrealizować na przykład prawa do przenoszenia czy prawa do usunięcia Pani/Pana danych.

H. PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO.

Gdy uzna Pani/Pan, iż przetwarzanie Pani/Pana danych osobowych narusza przepisy o ochronie danych osobowych, przysługuje Pani/Panu prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, z siedzibą w Warszawie, przy ul. Stawki 2, 00-193 Warszawa.

I. INFORMACJA O WYMOGU/DOBROWOLNOŚCI PODANIA DANYCH ORAZ KONSEKWENCJACH NIEPODANIA DANYCH OSOBOWYCH.

1. Podanie przez Panią/Pana danych osobowych może stanowić wymóg ustawowy, umowny bądź być warunkiem zawarcia umowy, a podanie danych być niezbędne dla określonego celu.
2. Jeśli nie poda Pani/Pan danych wymaganych ustawą, Administrator nie będzie mógł zrealizować wynikającego z ustawy obowiązku, co może skutkować w szczególności brakiem możliwości Pani/Pana udziału w postępowaniu o udzielenie zamówienia, a także innymi konsekwencjami przewidzianymi przepisami prawa.
3. Jeśli nie poda Pani/Pan danych wymaganych umową, nie będziemy mogli zawrzeć takiej umowy.
4. W przypadku, gdy będzie istniał wymóg umowny, a nie poda Pani/Pan swoich danych, nie będzie możliwości wykonania takiej umowy.

J. ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI, PROFILOWANIE

Nie będzie Pani/Pan podlegać decyzji, która opierała się będzie wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które jednocześnie będzie wywoływała wobec Pani/Pana skutki prawne lub w podobny sposób istotnie na Panią/Pana wpływało.

Łojzanta Gottwald
Zastępca Naczelnika
Wydziału Oświaty

.....
Podpis Naczelnika Wydziału

głowa

Załącznik nr 1

.....
Pieczęć Wykonawcy

FORMULARZ OFERTOWY

do Zapytania ofertowego z dnia 09.11.2022 r.

1. Oferta złożona w drodze zapytania ofertowego o udzielenie zamówienia publicznego na:
Dostawę 100 laptopów do szkół podstawowych oraz ponadpodstawowych w Zabrzu w ramach projektu pn. „Wsparcie dla uczniów z Ukrainy- MIASTO ZABRZE”
2. Nazwa i adres Wykonawcy, nr Regon/ PESEL, NIP, telefon, e-mail:
.....
.....
.....
3. Cena ofertowa zamówienia:
Cena Brutto:.....PLN
(słownie.....) w tym:
Cena netto:.....PLN
VAT.....PLN, tj. %
4. Osobą upoważnioną do kontaktu z Zamawiającym w sprawach dotyczących realizacji zlecenia jest:
.....
.....
(imię i nazwisko, tel. kontaktowy, e-mail)
5. Termin realizacji zamówienia: zgodnie z Zapytaniem ofertowym.
6. Warunki płatności: zgodnie z Zapytaniem ofertowym.
7. Termin związania ofertą: zgodnie z Zapytaniem ofertowym.
8. Oświadczam, że realizując przedmiotowe zamówienie będę w pełnym zakresie przestrzegać przepisów rozporządzenia Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) zwanego dalej w skrócie „**RODO**”¹⁾, w szczególności zapewniam wystarczające gwarancje wdrożenia odpowiednich środków technicznych

i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

☐

TAK

☐

NIE

Uwaga: W przypadku braku powyższej deklaracji bądź zaznaczenia wariantu „NIE” oferta Wykonawcy zostanie odrzucona na podstawie § 5 ust. 12 ppkt. 2 niniejszego Regulaminu jako niespełniająca warunków przedmiotu zamówienia.

9. Niniejszym oświadczam, że:

- a) Oferta obejmuje całość zamówienia;
- b) Cena ofertowa obejmuje wszystkie koszty związane z realizacją zamówienia;
- c) Zapoznałem się z warunkami zamówienia i nie wnoszę zastrzeżeń;
- d) Spełniam wszystkie warunki zawarte w Zapytaniu ofertowym,
- e) W razie wybrania mojej oferty zobowiązuję się do podpisania umowy na warunkach zawartych w Zapytaniu ofertowym;
- f) Oświadczam, że wypełniłem/ am obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO²⁾ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie niniejszego zamówienia.

10. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy p.z.p.

11. Do oferty załączam:

- a) Załącznik nr 2 do Zapytania ofertowego- Kalkulację ceny;
- b) Oświadczenie dotyczące podatku VAT (w przypadku zastosowania stawki innej niż 23%);
- c) Inne (wymienić)

.....dnia,

.....
Podpis wraz z pieczęcią osoby uprawnionej
do reprezentowania Wykonawcy

KIEROWNIK REFERATU
DS. REALIZACJI PROJEKTÓW
EDUKACYJNYCH

Zastępca Naczelnika
Wydziału Oświaty

dr Izabela Gottwald

²⁾ rozporządzenia Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2)

Kalkulacja ceny

dotyczy Zapytania ofertowego z dnia 09.11.2022 r.

Nazwa zamówienia: Dostawa 100 laptopów do szkół podstawowych oraz ponadpodstawowych w Zabrzu w ramach projektu pn. „Wsparcie dla uczniów z Ukrainy- MIASTO ZABRZE”

Nazwa i adres Wykonawcy NIP..... REGON.....

| Nazwa podzespołu/parametry | Opis minimalnych wymagań | Opis parametrów sprzętu oferowanego (równoważnego) |
|----------------------------|---|---|
| | komputer przenośny/notebook | (wpisać nazwę rynkową oferowanego sprzętu) |
| Ekran | 15.6" LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową, nie dopuszcza się matrycy typu "glare". Kłapa komputera otwierana do 180 stopni. | |
| Wydajność komputera | Oferowany komputer przenośny musi osiągać w teście wydajności : PC Mark 10 – wynik min. 3200 – test z przeprowadzonej konfiguracji załączyć do oferty. Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowanie overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). | |
| Chipset | Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora. | |
| Obudowa | Dopuszczalne kolory – czarny/srebrny. | |



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



| | |
|---------------------------------------|--|
| Pamięć RAM | Min. 16GB DDR4 (pamięć RAM rozszerzalna do 32GB – nie dopuszcza się wlotowanych pamięci w płytę główną). |
| Dysk twardy | Min. 256GB SSD Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.: - systemu operacyjnego - oprogramowania antywirusowego Partycja musi zapewnić przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania. Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5. |
| Karta graficzna | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana. |
| Karta dźwiękowa | Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz dwa cyfrowe mikrofony |
| Wbudowane połączenia i karty sieciowe | Karta sieciowa LAN 10/100/1000 LAN WLAN 802.11 ax wraz z Bluetooth 5.0 |
| Porty/złącza (wbudowane) | Min. 1x Złącze RJ-45 (podłączenie sieci lokalnej) Min. 1x Czytnik Kart pamięci SD Min. 1x USB-C 3.2 (z możliwością ładowania baterii laptopa) Min. 3x USB 3.2 Min. 1x VGA Min. 1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo) Min. 1x HDMI ze wsparciem HDCP Min. 1x zasilanie DC-in |
| Klawiatura | Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy). |
| Urządzenie wskazujące | Touch Pad (płytką dotykowa) wbudowana w obudowę notebooka. Czytnik linii papilarnych |



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



| | | |
|------------------------|--|--|
| Kamera | Wbudowana, o parametrach: HD 1280x720, 720p HD audio/video nagrywanie. Wbudowane dwa kierunkowe mikrofony. Mechaniczna przesłona kamery. | |
| Bateria | Litowo-jonowa 48Whr – czas pracy min. 10h wyników testów BAPCO MobileMark 25 – test załączyć do oferty. | |
| Zasilacz | Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 90W. | |
| Obudowa waga i wymiary | Waga nie większa niż 1,8kg, wysokość nie przekraczająca 20mm. Obudowa wzmocniona, szkielec wykonany ze wzmocnionego aluminium. Obudowa musi spełniać standard MIL-STD 810G (potwierdzony w oficjalnych dokumentach producenta lub załączonym wynikiem z przeprowadzonych testów) | |
| Bezpieczeństwo | <ul style="list-style-type: none">- Zabezpieczenie BIOS hasłem użytkownika.- Zabezpieczenie dysku twardego hasłem użytkownika.- Złącze typu Kensington Lock.- Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego - Trusted Platform Module 2.0. | |
| Gwarancja | Gwarancja producenta komputera min. 36 miesięcy Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie potwierdzające, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego producenta (oświadczenie należy dołączyć do oferty). Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera. Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001 Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 20:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych). | |



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



| | |
|--|---|
| <p>System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</p> | <p>System operacyjny Windows 11 Professional lub równoważny, musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none">1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<ol style="list-style-type: none">a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim4. Możliwość tworzenia pulpitu wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przelączenie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim9. Wbudowany system pomocy w języku polskim.10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. |
|--|---|



13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
24. Wbudowany mechanizm wirtualizacji typu hypervisor."
25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
27. Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
34. Możliwość tworzenia wirtualnych kart inteligentnych.
35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
38. Mechanizmy logowania w oparciu o:
- a. Login i hasło,
- b. Karty inteligentne i certyfikaty (smartcard),



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



| | | |
|--|--|--|
| | <p>c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</p> <p>d. Certyfikat/Klucz i PIN</p> <p>e. Certyfikat/Klucz i uwierzytelnienie biometryczne</p> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń</p> | |
| Certyfikaty i standardy | <p>Certyfikat ISO 9001, 14001, 50001 dla producenta sprzętu (należy załączyć do oferty).</p> <p>Deklaracja zgodności CE i ROHS (załączyć do oferty).</p> <p>Standard MIL-STD-810G (potwierdzony w oficjalnych dokumentach producenta lub załączonym wynikiem z przeprowadzonych testów)</p> | |
| Oprogramowanie zabezpieczające – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | <p>System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB ++, AV Comparative Advance +. Silnik musi umożliwiać co najmniej:</p> <ul style="list-style-type: none">• wykrywanie i blokowanie plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,• wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,• wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) <p>Szyfrowanie danych:</p> <ul style="list-style-type: none">• Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. | |



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



- Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.
- Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
- Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
- Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
- Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
- Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
- Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
- Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.
- Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające przez niezamierzonymi manipulacjami – ataki ransomware.
- Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:
 - Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



- Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.
 - Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
 - Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji Zarządzanie przez Chmury:
 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach
 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury
 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur
 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy
 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach
 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej
- Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.

1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer

2. Oprogramowanie klienckie, zarządzane z poziomu serwera.

System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:

- różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
- funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
- funkcje regulowania połączeń WiFi i Bluetooth
- funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
- funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi
- funkcje blokowania dostępu dowolnemu urządzeniu
- możliwość tymczasowego dodania dostępu do urządzenia przez administratora
- zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
- możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
- możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
- możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich
- funkcję wirtualnej klawiatury
- możliwość blokowania każdej aplikacji
- możliwość zablokowania aplikacji w oparciu o kategorie
- możliwość dodania własnych aplikacji do listy zablokowanych



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



- zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach Klientach poprzez konsolę administracyjną na serwerze
- dodawanie innych aplikacji
- dodawanie aplikacji w formie portable
- możliwość wyboru pojedynczej aplikacji w konkretnej wersji
- dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
- kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
- możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
- możliwość zablokowania funkcji Printscreen
- funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx
- funkcje monitorowania i kontroli przepływu poufnych informacji
- możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
- możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
- możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
- ochronę przed wyciekami informacji na drukarki lokalne i sieciowe
- ochrona zawartości schowka systemu
- ochrona przed wyciekami informacji w poczcie e-mail w komunikacji SSL
- możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
- ochrona plików zamkniętych w archiwach
- Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekami
- możliwość tworzenia profilu DLP dla każdej polityki



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



- wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
 - ochrona przez wyciekami plików poprzez programy typu p2p
- Monitorowanie zmian w plikach:
- Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
 - Funkcje monitorowania określonych rodzajów plików.
 - Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
 - Generator raportów do funkcjonalności monitora zmian w plikach.
 - możliwość śledzenia zmian we wszystkich plikach
 - możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
 - możliwość definiowania własnych typów plików
- Optymalizacja systemu operacyjnego stacji klienckich:
- usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
 - optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
 - możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
 - instruktaż stanowiskowy pracowników Zamawiającego
 - dokumentacja techniczna w języku polskim
- Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:
- Wymagania dotyczące technologii:
1. Dostęp do rozwiązań realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową



2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.
 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:
 - Microsoft Internet Explorer
 - Microsoft Edge
 - Mozilla Firefox
 - Google Chrome
 - Safari
 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących
 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
 6. Portal zarządzający musi umożliwiać:
 - a) przegląd wybranych danych na podstawie konfigurowalnych widgetów
 - b) zablokowania możliwości zmiany konfiguracji widgetów
 - c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
 - d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
 - e) eksport wszystkich skanów podatności do pliku CSV
- Backup i przywracanie danych
- Deduplikacja danych,
 - Backup przyrostowy i różnicowy,
 - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
 - Backup danych lokalnych – plikowy oraz poczty Outlook,
 - Backup otwartych plików (VSS),
 - Filtr plików oraz folderów,
 - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),
 - Wyłączanie komputera po wykonaniu backupu,



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



| | |
|--------------------------------|--|
| | <ul style="list-style-type: none">- Przywracanie danych do wskazanej lokalizacji,- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,- Wyszukiwanie plików w repozytorium użytkownika, <p>Ustawienia</p> <ul style="list-style-type: none">- Automatyczne logowanie,- Zapamiętywanie danych logowania,- Automatyczne uruchamianie programu przy starcie systemu,- Ustawianie priorytetu dla procesu backupu,- Zmiana klucza szyfrującego,- Ustawienia przepustowości/zajętości pasma,- Konfiguracja wydajności procesu backupu, <p>Bezpieczeństwo</p> <ul style="list-style-type: none">- Zastępowanie nazwy pliku GUID-em,- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,- Kompresja danych,- Transmisja po bezpiecznym protokole TLS,- Deklaracja klucza szyfrującego dane użytkownika,- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,- Obliczanie sumy kontrolnej,- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski. <p>WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS, Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczony jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.</p> |
| Wsparcie techniczne producenta | <p>A) Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.</p> |



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz Społeczny



| | | |
|--|---|--|
| | <p>B) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera.</p> <p>C) W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji.</p> | |
|--|---|--|

Koszt oferowanego ww. sprzętu:

| | 1 sztuka | 100 sztuk | uwagi |
|-------------|----------|-----------|-------|
| Cena netto | | | |
| VAT % | | | |
| VAT kwota | | | |
| Cena brutto | | | |

Oferowana cena brutto całości zamówienia: PLN (słownie.....)

.....
miejscowość i data

Kierownik Referatu

Beata Kobylnicka

KIEROWNIK REFERATU
DS. REALIZACJI PROJEKTÓW Zastępca Naczelnika
WYDZIAŁU OŚWIATY

Ingr Beata Szuran

dr Jolanta Gottwald

.....
podpis wraz pieczęcią osoby uprawnionej
do reprezentowania Wykonawcy