



Cyberbezpieczny Samorząd

Znak sprawy: ZP.271.14.2024.2

Mirsk, dnia 05.07.2024r.

Zapytanie ofertowe

Postępowanie prowadzone na podstawie § 5 ust. pkt 1) Regulaminu udzielania zamówień publicznych w Urzędzie Miasta i Gminy Mirsk wydatkowanych w zakresie realizacji projektów współfinansowanych ze środków UE.

1. Zamawiający: **Gmina Mirsk**

Adres korespondencyjny: pl. Wolności 39, 59-630 Mirsk

Tel. 75 64 70 440, e-mail: gmina@mirsk.pl

Zaprasza do złożenia oferty cenowej na:

Cyberbezpieczna Gmina Mirsk Zadanie 1 i Zadanie 2 dla zadania realizowanego z projektu grantowego **Finansowane z Funduszu Europejskiego na Rozwój Cyfrowy (FERC) Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmacnianie krajowego systemu cyberbezpieczeństwa, Europejski Fundusz Rozwoju Regionalnego (EFRR), Numer naboru FERC.02.02-CS.01-001/23**

2. Opis przedmiotu zamówienia

Zamówienie obejmuje dwa obszary działania w ramach realizacji zadania Cyberbezpieczna Gmina Mirsk. Przedmiot zamówienia będzie realizowany dla Urzędu Miasta i Gminy Mirsk, Zakładu Gospodarki Komunalnej i Mieszkaniowej w Mirsku, a także Miejsko Gminnego Ośrodka Pomocy Społecznej w Mirsku.

3. Przewidywany podział na części:

Zadanie 1 - Część 1 Obszar organizacyjny: Przedmiotem zamówienia dla Części 1 jest usługa wykonania wstępnego audytu bezpieczeństwa informacji dla Zamawiającego oraz wsparcie w wypełnieniu „Ankiety dojrzałości Cyberbezpieczeństwa”, która stanowi załącznik nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”. Następnie Wykonawca zrealizuje wdrożenie w Urzędzie Miasta Gminy Mirsk, a także podległych jednostkach organizacyjnych systemu zarządzania bezpieczeństwem informacji (SZBI). Dokumentacja SZBI musi obejmować bezpieczeństwo fizyczne (ochrona pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież,



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

nieuprawniony dostęp), bezpieczeństwo technologiczne (bezpieczeństwo systemu teleinformatycznego) oraz bezpieczeństwo osobowe i organizacyjne. Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;*
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023;
- Norma PN-EN ISO/IEC 22301:2020.

W ramach zadania Wykonawca opracuje oddzielny system dla każdej jednostki, który będzie obejmował m.in. wdrożenie dokumentacji, w tym niezbędnych polityk, procedur i instrukcji, przeprowadzenie szkolenia zespołu wdrożeniowego Zamawiającego w zakresie systemu zarządzania bezpieczeństwem informacji oraz zapewnienie wsparcia dla zespołu wdrożeniowego SZBI Zamawiającego.

Dodatkowo Wykonawca wykona okresowy audyt KRI (po wdrożeniu SZBI) zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Ustawą o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018r. (Dz. U. 2023 r. poz. 913), Normą ISO/IEC 27001, Normą PN-EN ISO/IEC 22301

Audyt ma obejmować weryfikację bezpieczeństwa:

- fizycznego (sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp)
- bezpieczeństwa informatycznego (analiza bezpieczeństwa systemu teleinformatycznego)
- bezpieczeństwa organizacyjnego (stosowanie procedur bezpieczeństwa), w tym przegląd dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji.

W ramach przeprowadzonych audytów Wykonawca przeprowadzi weryfikację:





Cyberbezpieczny Samorząd

- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji,
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
- zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,
- zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
- bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Wykonawca dostarczy Zamawiającemu:

- wstępnie wypełnioną „Ankiętę Dojrzałości Cyberbezpieczeństwa” oraz z finalnie uzupełnioną o stan i opis zrealizowanych zmian po zakończeniu zadania.
- raporty z audytów bezpieczeństwa informacji (dotyczy audytu wstępnego oraz okresowego) wraz z rekomendacjami do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.
- opracowany, opublikowany, zakomunikowany pracownikom i właściwym stronom zewnętrznym oraz aktualizowany na bieżąco zgodnie z zewnętrznymi wymaganiami System Zarządzania Bezpieczeństwem Informacji (SZBI).

Zadanie 2 - Część 2 Obszar kompetencyjny: Szkolenie pracowników i audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji z zakresu cyberbezpieczeństwa. Opracowanie kompleksowego programu szkoleniowego z zakresu cyberbezpieczeństwa w celu



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa wszystkich pracowników. Szkolenie audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji. Przeprowadzenie testów socjotechnicznych poprzez rozesłanie na adresy e-mail służbowe pracowników wiadomości pozorujących przeprowadzenie ataku socjotechnicznego. Audytor będzie mógł sprawdzić ilu pracowników otworzy linki sprawdzające oraz od ilu pracowników byłby w stanie uzyskać hasła dostępowe.

Szkolenia muszą być zrealizowane w siedzibie:

- Urzędu Miasta i Gminy Mirsk - Plac Wolności 39, 59-630 Mirsk
 - Zakładu Gospodarki Komunalnej i Mieszkaniowej w Mirsku – ul. A. Mickiewicza 38, 59-630 Mirsk
 - Miejsko Gminnego Ośrodka Pomocy Społecznej w Mirsku – Plac Wolności 40, 59-630 Mirsk
- Co najmniej 4 tury szkolenia dla każdej jednostki w wymiarze co najmniej 4 godzin każda oraz co najmniej po 2 próby testów socjotechnicznych i penetracyjnych dla każdej jednostki.**

4. Warunki udziału w postępowaniu:

- a. W okresie ostatnich 3 lat, zrealizował co najmniej cztery audyty cyberbezpieczeństwa (niewskazane w pkt. b, c, d) o wartości co najmniej 20 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzone referencjami;
- b. Zrealizował co najmniej dwa inne audyty bezpieczeństwa informacji (niewskazane w pkt. a, c, d) o wartości co najmniej 10 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzone referencjami;
- c. Wykonał co najmniej dwa projekty dotyczące szacowania ryzyka dla bezpieczeństwa danych w systemach informatycznych, potwierdzonych referencjami,
- d. Wykonał co najmniej dwa projekty polegające na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów publicznych.
- e. **Posiada zespół składający się z co najmniej 2 osób, w tym:**
 - minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie audytowania systemów zarządzania bezpieczeństwem informacji przy spełnieniu wymagań dla audytorów IRCA, CQI lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości,





Cyberbezpieczny Samorząd

potwierdzone certyfikatem ukończenia kursu Information Security Management Systems Auditor (ISMS) lub innym równoważnym dokumentem (zaświadczeniem);

- minimum 1 osobą posiadającą aktualne uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
- minimum 1 osobą posiadającą kompetencje w zakresie audytowania systemów zarządzania ciągłością działania przy spełnieniu wymagań dla audytorów wiodących Systemu Zarządzania Ciągłością Działania zgodnego z normą PN-EN ISO 22301 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla Audytora Wiodącego Systemu Zarządzania Ciągłością Działania zgodnego z normą PN-EN ISO 22301 po zdaniu egzaminu lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą kompetencje w zakresie audytowania systemów zarządzania jakością przy spełnieniu wymagań dla audytorów wewnętrznych Systemu Zarządzania Jakością zgodnego z normą PN-EN ISO 9001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla Audytora Wewnętrznego Systemu Zarządzania Jakością zgodnego z normą PN-EN ISO 9001 po zdaniu egzaminu lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie wdrażania systemów zarządzania bezpieczeństwem informacji zgodnie z normą ISO 27001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem) oraz uczestniczącą w projektach wdrożenia systemu zarządzania bezpieczeństwem informacji na podstawie Rozporządzenia KRI w przynajmniej dwóch podmiotach publicznych;
- minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie ryzyka w ochronie informacji potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą, która uczestniczyła w co najmniej 2 projektach dotyczących zarządzania ryzykiem w bezpieczeństwie informacji, w tym w co najmniej 1 projekcie dotyczącym zarządzania ryzykiem na podstawie normy ISO 27005.





Cyberbezpieczny Samorząd

- minimum 1 osobą posiadającą wiedzę w zakresie wymagań *Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą, która przeprowadziła co najmniej 10 szkoleń w zakresie cyberbezpieczeństwa / bezpieczeństwa informacji / ochrony danych dla podmiotów publicznych;
- minimum 1 osobą posiadającą wiedzę w zakresie zarządzania cyberbezpieczeństwem potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą wiedzę w zakresie administrowania sieciami teleinformatycznymi, potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem).
- minimum 1 osobą, która odbyła specjalistyczne szkolenie w zakresie cyberbezpieczeństwa, na podstawie norm ISO 27001, 22301 i przepisów RODO, potwierdzone certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem).

5. Przedmiot zamówienia opisany został wg następujących kodów CPV:

- 80500000-9: Usługi szkoleniowe
- 80511000-9: Usługi szkolenia personelu
- 72000000-5: Usługi informacyjne, konsultacje, opracowania, internetowe i wsparcia
- 72810000-1: Usługi audytu komputerowego
- 72300000-8: Usługi w zakresie danych
- 72316000-3: Usługi analizy danych
- 72315000-6: Usługi zarządzania siecią danych oraz usługi wspierające
- 72240000-9: Usługi analizy systemu i programowania
- 72224200-3: Usługi w zakresie planowania zapewnienia jakości systemu
- 72223000-4: Usługi w zakresie wymogów technologii informacji
- 72222000-7: Usługi w zakresie systemów informatycznych lub strategicznej analizy technologicznej oraz usługi w zakresie planowania





Cyberbezpieczny Samorząd

- 72222100-8: Usługi w zakresie systemów informatycznej lub strategicznej analizy technologicznej
6. Wykonawca związany jest ofertą 60 dni.
7. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
8. Szacunkowy termin wykonania zamówienia:
- a) „Ankieta Dojrzałości Cyberbezpieczeństwa” do **24.07.2024r.**
 - b) Pozostałe części zamówienia zgodnie z przedstawionym przez Wykonawcę i zaakceptowanym przez Zamawiającego harmonogramem jednak nie później niż do dnia **31.03.2026r.**
9. Dokumenty, jakie Wykonawca powinien załączyć do oferty: **W celu wykazania spełnienia warunków udziału w postępowaniu, Wykonawca wraz z ofertą musi dostarczyć:**
- Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej czterech audytów cyberbezpieczeństwa (niewskazanych w odpowiedzi na wymóg w ust. II pkt. b, c, d), w ciągu ostatnich 3 lat, o wartości co najmniej 20 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzony referencjami;
 - Referencje lub inny dokument potwierdzający prawidłowe wykonanie, co najmniej dwóch, innych audytów bezpieczeństwa informacji (niewskazanych w odpowiedzi na wymóg ust. II pkt. a, c, d) o wartości co najmniej 10 000,00 zł brutto, w podmiocie realizującym zadania publiczne;
 - Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej dwóch projektów dotyczących szacowania ryzyka dla bezpieczeństwa danych w systemach informatycznych, w tym w co najmniej 1 projekcie dotyczącym zarządzania ryzykiem na podstawie normy ISO 27005;
 - Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej dwóch projektów polegających na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów publicznych;
 - Co najmniej jeden certyfikat ukończenia kursu Information Security Management Systems Auditor (ISMS);





Cyberbezpieczny Samorząd

- Co najmniej 1 aktualny certyfikaty wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
 - Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301;
 - Co najmniej 1 certyfikat Audytora Wewnętrznego Systemu Zarządzania Jakością według normy PN-EN ISO 9001;
 - Certyfikat/ zaświadczenie ukończenia szkolenia w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji wg ISO 27001;
 - Certyfikat/ zaświadczenie ukończenia szkolenia w zakresie ryzyka w ochronie informacji;
 - Certyfikat ukończenia szkolenia w zakresie wymagań Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
 - Referencje za przeprowadzenie co najmniej 10 szkoleń w zakresie cyberbezpieczeństwa / bezpieczeństwa informacji / ochrony danych dla podmiotów publicznych;
 - Certyfikat ukończenia szkolenia w zakresie zarządzania cyberbezpieczeństwem;
 - Certyfikat ukończenia szkolenia w zakresie administrowania sieciami teleinformatycznymi;
 - Zaświadczenie o odbyciu specjalistycznego szkolenia w zakresie cyberbezpieczeństwa na podstawie norm ISO 27001, 22301 i przepisów RODO;
10. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów.
- e-mailem na adres: **gmina@mirsk.pl** ,
 - Adres Elektronicznej Skrzynki Podawczej Gminy Mirsk: **/s0eka1s21o/SkrytkaESP**
11. Osoby po stronie Zamawiającego uprawnione do porozumiewania się z Wykonawcami:
- Jan Zaliwski – Sekretarz Gminy Mirsk, email: sekretarz@mirsk.pl tel. 756470442 – przedmiot zamówienia.
 - Alicja Jaszczyszyn – Inspektor ds. ochrony danych osobowych i zamówień publicznych, email: rodo@mirsk.pl, tel. 75 62 22 169 – procedura udzielania zamówienia.
12. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie istotnych warunków udzielenia zamówienia w godzinach pracy urzędu tj.: od poniedziałku do piątku w godz. 7³⁰-15³⁰.





Cyberbezpieczny Samorząd

13. Miejsce, termin oraz sposób składania ofert:

- Oferta powinna zostać złożona do terminu otwarcia ofert, czyli do dnia **12.07.2024r.**, godziny 11:00.
- Oferent może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
- W toku badania i oceny ofert Zamawiający może żądać od oferentów wyjaśnień.
- Zamawiający umożliwia składanie ofert: e-mailem na adres: gmina@mirsk.pl lub Adres Elektronicznej Skrzynki Podawczej Gminy Mirsk: /s0eka1s21o/SkrytkaESP w tytule należy wpisać: **oferta na zadanie: „Cyberbezpieczna Gmina Mirsk Zadanie 1 i Zadanie 2.**

14. Kryteria oceny ofert - **Cena 100%**

Punktacja i ocena ofert zostanie wyliczona w oparciu o ustalone kryteria, wg wyliczeń przedstawionych poniżej:

$$\frac{\text{Cena najniższa ze wszystkich ofert} \times 100\text{pkt} \times \text{Znaczenie kryterium } 100\%}{\text{Cena oferty badanej}}$$

Cena oferty badanej

Oferta może otrzymać maksymalnie 100 pkt (1% = 1 pkt) w zakresie kryterium ceny.

15. Opis sposobu obliczania ceny

- 1) Na załączonym formularzu cenowo-ofertowym, należy przedstawić cenę ofertową brutto za wykonanie /udzielenie przedmiotu zamówienia.
- 2) Wartość cenową należy podać w złotych polskich, cyfrą – z dokładnością do dwóch miejsc po przecinku oraz słownie.
- 3) Cena powinna zawierać wszelkie koszty związane z wykonaniem przedmiotu zamówienia.
- 4) Wszelkie rozliczenia pomiędzy Zamawiającym a Wykonawcą odbywać się będą w polskich złotych.

16. Informacje o formalnościach

- 1) Od Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, wymagane będzie wniesienie, przed zawarciem umowy, zabezpieczenia należytego wykonania umowy w wysokości **3 % ceny całkowitej (brutto)** podanej w ofercie za wykonanie całości przedmiotu zamówienia. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
- 2) Zamawiający zwróci zabezpieczenie w następujących terminach:



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTSUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

70% wysokości zabezpieczenia w terminie 30 dni od dnia podpisania protokołu odbioru końcowego przedmiotu zamówienia, tj. od dnia wykonania zamówienia i uznania przez zamawiającego za należyte wykonane;

30% wysokości zabezpieczenia w terminie 15 dni od dnia, pozytywnej weryfikacji wniosku rozliczającego projekt grantowy **przez Granatowce – Skarb Państwa, w imieniu którego działa Centrum Projektów Polska Cyfrowa.**

- 3) Zabezpieczenie powinno zostać wpłacone przelewem na rachunek bankowy zamawiającego w banku PKO BP S.A. numer rachunku: **58 1020 2124 0000 8102 0011 1468**, tytuł przelewu: „**Cyberbezpieczna Gmina Mirsk Zadanie 1 i Zadanie 2**”.
- 4) Zamawiający zawrze umowę z wybranym Wykonawcą po przekazaniu zawiadomienia o wyborze Wykonawcy, ale nie później niż w terminie związania ofertą.
- 5) Jeżeli Wykonawca, którego oferta została wybrana uchyli się od zawarcia umowy, Zamawiający wybierze kolejną ofertę najkorzystniejszą spośród złożonych ofert, bez przeprowadzenia ich ponownej oceny.
- 6) Niniejsze postępowanie prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach organizacyjnych Zamawiającego. Nie mają w tym przypadku zastosowania przepisy ustawy z dnia 11 września 2019r. - Prawo zamówień publicznych.
- 7) Zamawiający może odstąpić od udzielenia zamówienia bez podania jakichkolwiek przyczyn.

Załączniki:

1. Formularz cenowo-ofertowy
2. Wzór umowy

Zatwierdził:

BURMISTRZ
Miasta i Gminy Mirsk
Andrzej Jasiński

Sprawę prowadzi:
Inspektor ds. ochrony danych osobowych
i zamówień publicznych
Alicja Jaszczyżyn
tel. 75 62 22 169, e-mail: rodo@mirsk.pl



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA