**ИЗИСКВАНИЯ ЗА ИКОНОМИЧЕСКОТО И ФИНАНСОВО СЪСТОЯНИЕ И ТЕХНИЧЕСКИТЕ ВЪЗМОЖНОСТИ И/ИЛИ КВАЛИФИКАЦИЯ НА УЧАСТНИЦИТЕ**

обособена позиция „Проверка и анализ на киберсигурността на информационните системи на Министерство на външните работи чрез контролирани опити за проникване през периметъра и тестове за откриване и експлоатиране на уязвимости и слабости на корпоративната мрежа, инфраструктурни услуги и сървърната инфраструктура на министерството“

1. **Изисквания за годност (правоспособност) за упражняване на професионална дейност на участниците:**

Неприложимо

1. **Икономическо и финансово състояние на участниците**

Неприложимо

1. **Изисквания към техническите и професионалните способности на участниците**
   1. **Опит в изпълнението на доставки/услуги, идентични или сходни с предмета на поръчката**
      1. Участникът да е изпълнил минимум 1 (една) дейност с предмет, идентичен или сходен с предмета на поръчката през последните три години, считано от датата на подаване на офертата.

Под „дейност, сходна с предмета на обществената поръчка“ следва да се разбира дейност за проверка и анализ на сигурността на информационни системи и/или информационна инфраструктура и/или софтуерни приложения, с използване на офанзивни методи за тестване на сигурността.

Възложителят не изисква обем на доставката.

***Забележка*:** *„Изпълнена“ е тази дейност, която е приключила в рамките на 3-годишния период преди датата на подаване на офертата, независимо от датата на възлагането на услугата и резултатът от нея е надлежно приет от възложителя.*

Информация за опита на участника се попълва в Част IV, Раздел В, за поръчки за доставки: извършени доставки от конкретния вид“ от еЕЕДОП.

Съответствието с минималните изисквания по т. 3.1.1. от този раздел относно опит в изпълнението на доставки, идентични или сходни с предмета на поръчката, се установява съгласно чл. 64, ал. 1, т. 2 ЗОП.

* + 1. Участникът трябва да притежава валидно Удостоверение за сигурност (УС) минимум до ниво „Поверително!“. Същото следва да се с валидност не по-малка от 6 месеца след датата на подаване на заявлението за участие в процедурата.

За доказване на посоченото изискване участникът предоставя заверено копие на валидно УС минимум до ниво „Поверително“

* + 1. Участникът следва да разполага със сертифицирана Регистратура за обработка и съхранение на национална класифицирана информация (РКИ) минимум до ниво „Поверително“

За доказване на посоченото изискване участникът предоставя заверено копие от Сертификата на РКИ минимум до ниво „Поверително!“

* 1. **Изисквания към стандарти за осигуряване на качеството и стандарти за екологично управление** 
     1. Участникът следва да прилага система за управление на качеството, съответстваща на стандарт БДС ЕN ISO 9001:2015 или еквивалентен, сходен с предмета на поръчката. Поставеното изискване се доказва с документ по чл. 64, ал. 1, т. 10 от ЗОП – сертификат, издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция "Българска служба за акредитация" или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието. Възложителят приема еквивалентни сертификати, издадени от органи, установени в други държави членки.

Участниците трябва да декларират съответствието си с изискването като посочат в Част IV, Раздел Г – „Стандарти за осигуряване на качеството и стандарти за екологично управление“ от еЕЕДОП: номер на сертификата, предметният му обхват, датата на издаването му, датата, до която е валиден и организацията, издала сертификата.

За установяване на съответствие с изискванията към стандарти за осигуряване на качеството и стандарти за екологично управление, избраният за изпълнител участник представя копие от сертификат за управление на качеството съгласно стандарт БДС ЕN ISO 9001:2015 или еквивалентен с обхват, сходен с предмета на поръчката. Когато участникът не е имал достъп до такъв сертификат или е нямал възможност да го получи в съответните срокове по независещи от него причини, той може да представи други доказателства за еквивалентни мерки за осигуряване на система за управление на качеството. В тези случаи участникът трябва да е в състояние да докаже, че предлаганите мерки са еквивалентни на изискваните.

* + 1. Участникът трябва да прилага сертифицирана система за управление на ИТ услуги, съответстваща на стандарт EN ISO/IEC 20000-1:2011 или еквивалентен с обхват, сходен с предмета на поръчката.

За доказване на посоченото изискване участникът трябва да представи към техническото предложение копие на валиден сертификат за въведена система за управление на услугите съгласно стандарта EN ISO/IEC 20000-1:2011 или еквивалентен с обхват, сходен с предмета на поръчката.

* + 1. Участникът трябва да прилага сертифицирана система за управление на сигурността на информацията, съответстваща на стандарт EN ISO/IEC 27001:2013 или еквивалент, с обхват сходен с предмета на поръчката.

За доказване на посоченото изискване участникът трябва да представи към техническото предложение копие на валиден сертификат за въведена система за управление на сигурността на информацията съгласно стандарта EN ISO/IEC 27001:2013 или еквивалентен, с обхват сходен с предмета на поръчката.

* 1. **Минимални изисквания към персонала/екипа за изпълнение на поръчката**

Участникът трябва да разполага с квалифициран екип за изпълнение на поръчката, който да включва най-малко следните видове експерти:

* + 1. Ключов експерт 1: „Ръководител на проекта“ - минимум 1 експерт

Участникът следва да разполага минимум с един ключов експерт – ръководител на проекта за целите на обезпечаване гарантиране изпълнението на проекта в съответствие с международно утвърдени добри практики, с минимални изисквания, както следва:

* Образование: Висше образование, образователно-квалификационна степен „магистър” в една от следните области и професионални направления: област „Природни науки, математика и информатика“ с професионални направления "Информатика и компютърни науки" или "Математика", област „Социални, стопански и правни науки“ с професионални направления „Администрация и управление“ или „Икономика“ или област „Технически науки“ с професионални направления "Комуникационна и компютърна техника" (съгласно Класификатора на областите на висшето образование и професионалните направление, утвърден с ПМС № 125 от 2002 г.) или еквивалентна образователна степен, когато е придобита в чужбина, в еквивалентни на посочените професионални направления – *доказва се с копие от диплома*;
* Професионален опит: минимум 10 (десет) години практически опит в областта на информационната сигурност; минимум 5 (пет) години практически опит в областта на управлението на дейности за разработка/развитие, внедряване и поддръжка на информационни системи; ръководител на минимум 2 /два/ проекта за разработка и/или развитие и поддръжка на информационни системи в държавната администрация които извършват машинен обмен на данни с други външни системи; участие като експерт в минимум в един проект за проверка и анализ на киберсигурността – *доказва се със сертификати, референции от работодател/възложител или по друг еквивалентен начин*;
* Сертификати: експертът трябва да притежава валиден международен сертификат за ръководител на проекти Project Management Professional и/или Prince2 Practitioner или еквивалентен и валиден сертификат Certified Information Systems Security Professional (CISSP) и/или Certified Chief Information Security Officer (CCISO) или еквивалентен – *доказва се със заверено копие от сертификат*
* Валидно Разрешение за достъп до класифицирана информация (РДКИ) минимум до ниво „Поверително“ – *доказва се със заверено копие от РДКИ.*
  + 1. Ключов експерт 2: „Експерт по информационна сигурност“ - минимум 1 експерт

Участникът следва да разполага с минимум един водещ експерт, който да комуникира всички технически въпроси и да извърши трансфер на знания към проектния екип на Възложителя, с минимални изисквания, както следва:

* Образование: Висше образование, образователно-квалификационна степен „бакалавър“ или „магистър” в една от следните области: „Природни науки, математика и информатика“ или „Технически науки“ с професионални направления "Комуникационна и компютърна техника" (съгласно Класификатора на областите на висше образование и професионалните направления, утвърден с ПМС № 125 от 2002 г.) или еквивалентна образователна степен, когато е придобита в чужбина, в области, еквивалентни на посочените– *доказва се с копие от диплома*;
* Професионален опит: минимум 7 /седем/ години практически опит в областта на информационните технологии, свързан с работа в областта на информационната сигурност и защита на данните; участие като експерт по информационна сигурност в минимум един проект за разработка и/или развитие и поддръжка на информационна система в държавната администрация, която извършва машинен обмен на данни с други външни системи – *доказва се със сертификати, референции от възложител/работодател или по друг еквивалентен начин*;
* Сертификати: експертът трябва да притежава валиден сертификат Certified Ethical Hacker, или Offensive Security Certified Professional, или Offensive Security Certified Expert или еквивалентен – *доказва се със заверено копие от сертификат или от отчет за сертификация*;
* Валидно РДКИ минимум до ниво „Поверително“ – *доказва се със заверено копие от РДКИ*.
  + 1. Ключов експерт 3: „Експерт информационни системи“ - минимум 1 експерт

Участникът следва да разполага с минимум един водещ експерт, който да комуникира всички технически въпроси и да извърши трансфер на знания към проектния екип на Възложителя, с минимални изисквания, както следва:

* Образование: Висше образование, образователно-квалификационна степен „бакалавър“ или „магистър” в една от следните области и професионални направления: област „Природни науки, математика и информатика“ с професионални направления "Информатика и компютърни науки" или област „Технически науки“ с професионални направления "Комуникационна и компютърна техника" (съгласно Класификатора на областите на висше образование и професионалните направления, утвърден с ПМС № 125 от 2002 г.) или еквивалентна образователна степен, придобита в чужбина, в еквивалентни на посочените професионални направления – *доказва се с копие от диплома*;
* Професионален опит: минимум 5 /пет/ години практически опит в областта на информационните технологии, свързан с работа по проекти за разработка/развитие, внедряване и поддръжка на информационни системи; участие като експерт в минимум един проект за разработка и/или развитие и поддръжка на информационна система в държавната администрация, която извършва машинен обмен на данни с други външни системи – *доказва се със сертификати, референции от възложител/работодател или по друг еквивалентен начин*;
* Сертификати: експертът трябва да притежава сертификат за работа с една или повече технологии за разработка на информационни системи, издаден от съответния производител или негов оторизиран център – *доказва се със заверено копие от сертификат или от отчет за сертификация*;
* Валидно РДКИ минимум до ниво „Поверително“ – *доказва се със заверено копие от РДКИ*.
  + 1. Ключов експерт 4: „Експерт по офанзивни методи за проникване в информационни системи и мрежи“ - минимум 1 експерт

Участникът следва да разполага с минимум един водещ експерт, който да комуникира всички технически въпроси и да извърши трансфер на знания към проектния екип на Възложителя, с минимални изисквания, както следва:

* Професионален опит: минимум 5 /пет/ години практически опит в областта на информационната сигурност; участие като експерт в минимум 2 (два) проекта за анализ на сигурността с използване на офанзивни методи за тестване на сигурността – *доказва се със сертификати, референции от възложител/работодател или по друг еквивалентен начин*;
* Сертификати: експертът трябва да притежава валиден сертификат Offensive Security Certified Professional, или Offensive Security Certified Expert или еквивалентен – *доказва се със заверено копие от сертификат или от отчет за сертификация*;
* Валидно РДКИ минимум до ниво „Поверително“ – *доказва се със заверено копие от РДКИ*.

***Забележка:*** *За изпълнение на изискванията за образование се приема и висше образование, придобито преди влизането в сила на ПМС № 125 от 2002 г., когато е в област и/или направление, едноименни/еквивалентни на посочените по-горе.*

Не се допуска едно лице да съвместява различни позиции, независимо че може да отговаря на изискванията, приложими за повече от една позиция в екипа.

Участниците трябва да декларират съответствието си с изискването по т.т. 3.3.1 до 3.3.3 от този раздел като посочат в Част IV, Раздел В – „образователна и професионална квалификация“ от еЕЕДОП следната информация за предлаганите технически лица:

* позиция в екипа;
* име, презиме и фамилия на лицето;
* образование;
* придобит стаж (когато е приложимо);
* притежавани сертификати (когато е приложимо);
* проекти/дейности, при изпълнението на които лицето е придобило изискуемия опит.

Съответствие с минималните изисквания по т. 3.2.1. от този раздел относно персонала/екипа за изпълнение на поръчката, се установява съгласно чл. 64, ал.1, т. 6 от ЗОП, при условията на чл. 67, ал. 5 и чл. 112, ал. 1, т. 2 от ЗОП.