ИЗИСКВАНИЯ

Относно: обществена поръчка с предмет: *„Подновяване на сертификата (ресертификация) на Системата за управление на сигурността на информацията и придобиване на сертификат за съответствие с изискванията на стандарт ISO/IEC 27001:2013, с валидност 3 (три) години"*

1. Изисквания към участниците:

1.1. Участникът трябва да притежава валидна акредитация, съгласно ISO/IEC 17021 или еквивалентен или EN 45011 или еквивалентен, издадена от международна организация по акредитация, (пълноправен член на Европейската организация за акредитация (ЕА) и/или орган по акредитация на друга държава. Обхватът на акредитацията следва да е съобразен с предмета на дейност на Възложителя.

За доказване на това изискване участникът представя заверено копие на сертификат/документ за акредитация (с подпис, печат и текст „Вярно с оригинала", вкл. с превод на бълг. език, ако е приложимо) с приложения, ако са налични, доказващи обхвата на акредитация.

1.2. Участникът да има сключена застраховка „Професионална отговорност", в съответствие с изискването на ISO/IEC 17021-1:2015, т. 5.3. „Отговорност и финансиране", 5.3.1 „Органът за сертификация трябва да има доказателство, че той е оценил значимите рискове, произтичащи от дейността му по сертификация, и че е взел подходящи мерки (например застраховка или резервен фонд) за покриване на задълженията в резултат на действията му във всяка област от дейността му и за всяка географска зона, където той работи" или еквивалент.

За доказване на това изискване участникът представя заверено копие на застраховка „Професионална отговорност" в съответствие с горепосоченото (с подпис, печат и текст „Вярно с оригинала", вкл. с превод на бълг. език, ако е приложимо).

1.3. Участникът трябва да е изпълнил дейности с предмет, идентичен или сходен с този на поръчката през последните 3 (три) години, считано от датата на подаване на офертата.

Изискано минимално ниво: Участникът следва да е изпълнил поне 1 (една) услуга с предмет, идентичен или сходен с този на поръчката през последните 3 (три) години от датата на подаване на офертата.

Под *„предмет, идентичен или сходен с предмета на поръчката"* следва да се разбира осъществяване на пълния обем на настоящата поръчка в организации от публичния сектор, аналогични като брой площадки/персонал.

За доказване на това изискване участникът представя списък на услугите с предмет, идентичен или сходен с този на поръчката през последните 3 (три) години, считано от датата на подаване на офертата, включващ посочване на предмет на услугата, начална и крайна дата на изпълнение, получател и стойност.

1.3.1. Участникът следва да разполага с персонал с определена професионална квалификация за изпълнение предмета на обществената поръчка, както следва:

-екип одитори, в достатъчен брой, съобразен с броя на площадките на Системата за управление и сроковете за изпълнение на поръчката, от които минимум 1 (един) с професионална квалификация на водещ одитор по международните стандарти, отговарящ на следните изисквания:

- да има валиден сертификат за водещ одитор на система за управление на информационната сигурност съгласно ISO/IEC 27001:2013 и ISO 19011:2011 или еквивалентни.

- да е имал участие в сертифициране (ресертифициране) и одит на Системи за управление на сигурността на информацията по ISO/IEC 27001:2013 на не по-малко от 1 (една) организация, независимо от нейния статут и предмет на дейност;

- да има най-малко 1 (една) година професионален опит в сферата на изпълнение на задачи по одит на Системи за управление.

За доказване на това изискване участникът представя списък с имената на членовете от одиторския екип, в т.ч. и на водещия одитор, с информация за тяхното образование, професионална квалификация и професионален опит, съобразно изискванията, както и заверено копие на валиден сертификат за водещ одитор на система за управление на информационната сигурност съгласно ISO/IEC 27001:2013 и ISO 19011:2011 или еквивалентни.

1.4 Специфични изисквания:

1.4.1.Всички одити на информационната система на „Български пощи" ЕАД извършвани от външни организации, независимо от това дали са за оценяване на съответствието от трета страна или в изпълнение на законови и/или договорни изисквания, се провеждат в съответствие с ISO/IEC 17021-1:2015 „Оценяване на съответствието. Изисквания към органите, извършващи одит и сертификация на системи за управление. Част 1: Изисквания". (или стандарт EN 45011, или еквивалентен).

1.4.1.1. При всеки одит от външна организация, независимо от целта на одита (сертификация, партньорска оценка или други одитни процеси), се прилагат критериите в ISO/IEC 27006:2015 „Информационни технологии - Техники за сигурност - Изисквания към органите, предоставящи одит и сертифициране на системи за управление на информационната сигурност", допълващ изискванията, съдържащи се в ISO/IEC 17021-1 и ISO/IEC 27001.

1.4.1.2.Прилага се изискването на ISO/IEC 27006:2015, т. 8.4.1 „Достъп до организационни записи", съгласно което одитиращата организация трябва да е поискала и получила от „Български пощи" ЕАД информация за това дали има системи, приложения и/или записи с информация или данни, които не могат да бъдат на разположение за проверка от одитния екип, тъй като съдържат поверителна или чувствителна информация.

1.4.2. С ПМС № 107 от 31 май 2022 год. за допълнение на ПМС № 181 от 2009 год. за определяне на стратегическите обекти и дейности, които са от значение за националната сигурност, „Български пощи" ЕАД е определен като стратегически обект.

В тази връзка:

1.4.2.1 „Български пощи" ЕАД изпълнява приложимите мерки, касаещи ИКТ системите на стратегическите обекти, съдържащи се в „Наредба за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяването на контрол" (В сила от 15.10.2019 г., Приета с ПМС № 256 от 10.10.2019 г., Обн. ДВ. бр.81 от 15 Октомври 2019г.), глава втора и глава трета.

1.4.2.2 Одитиращата организация сключва с „Български пощи" ЕАД договор с клауза за конфиденциалност или споразумение по сигурността на информацията, съдържащи изчерпателно описание на одитните процеси и представя на „Български пощи" ЕАД необходимата информация за професионалната компетентност на всеки одитор от одиторския екип (биографични данни и доказателства за професионална компетентност).

1.4.2.3 Членовете на одиторския екип подписват декларации за безпристрастност и опазване на търговската и производствена тайна по чл. 37, ал. 1 и ал. 2 от Закона за защита на конкуренцията.

1.4.2.4 Физически достъп на одиторския екип в стратегическата зона на стратегически обект „Български пощи" ЕАД не се предвижда.

1.4.2.5 Отдалечен достъп със софтуерен инструмент, ползван за целите на одита, собствен или нает от одитиращата организация и/или член от персонала/одитор от одиторския екип, не се допуска.

1.4.2.6 Одитни действия чрез наблюдение на системите за управление на информационната и комуникационна инфраструктура, бази данни и приложения, одиторския екип извършва само чрез и в присъствието на администратора на съответната система.

2. Критерий за възлагане:

Критерий за оценка е „икономически най-изгодната оферта" – „най-ниска цена".

3. Документи, изисквани към офертата:

Участникът трябва да представи следните документи:

3.1Образец на оферта; 3.2. План-график за изпълнението на дейността, включващ:

3.2.1. Описание на последователността и времевата продължителност на всички етапи, експерти, които ще работят през всеки един от етапите и съответните документи по изпълнение на дейностите. План-графикът следва ясно да посочва, че всички дейности по договора ще бъдат завършени в рамките на крайния срок за изпълнение, предложен от участника.

3.2.2. Срок за изпълнение на всички дейности по одита, включващ проверка и оценка на Системата за управление на сигурността на информацията и издаване на сертификат за съответствие с изискванията на стандарт ISO/IEC 27001:2013, не повече от 25 календарни дни, считано от датата на сключване на договора и писменото уведомяване на Изпълнителя от страна на Възложителя за готовността му да започне извършването на ресертификационен одит.

3.3. Заверено копие на сертификат/документ за акредитация с приложения, ако са налични, доказващи обхвата на акредитация.

3.4. Заверено копие на застраховка „Професионална отговорност" в съответствие с изискванията на Възложителя.

3.5. Списък на услугите с предмет, идентичен или сходен с този на поръчката през последните 3 (три) години, считано от датата на подаване на офертата, включващ посочване на предмет на услугата, начална и крайна дата на изпълнение, получател и стойност.

3.6. Списък с имената на членовете от одиторския екип, в т.ч. и на водещия одитор, с информация за тяхното образование, професионална квалификация и професионален опит, съобразно изискванията, както и заверено копие на валиден сертификат за водещ одитор на система за управление на информационната сигурност съгласно ISO/IEC 27001:2013 и ISO 19011:2011 или еквивалентни.

Забележка: Оферта, която не съдържа изброените по-горе документи, се отстранява от участие.