ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

Относно: *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.*

I. ПРЕДМЕТ

Предмет на поръчката е избор на изпълнител на дейности по *„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."*

Услугите за сертифициране трябва да бъдат извършени от Орган по сертификация, който е акредитиран съгласно стандарт ISO/IEC 17021 или EN 45011, или еквивалентен.

Сертифициращата организация следва да има акредитация от международна организация по акредитация, (пълноправен член на Европейската организация за акредитация (ЕА) и/или орган по акредитация на друга държава), за област *„Органи за сертификация на системи за управление"*

Услугите включват един ресертификационен одит и два надзорни одита, провеждани на едногодишни интервали, в рамките на тригодишен сертификационен срок, както следва:

1. Провеждане на ресертификационен одит, включващ проверка и оценка на Системата за управление на сигурността на информацията, съгласно изискванията на стандарт ISO/IEC 27001:2013, разширен до ISO 27701:2019, ISO/IEC 27017:2015, ISO/IEC 27018:2019 до м. октомври 2023

2. Провеждане на първи надзорен одит, включващ проверка и оценка на Системата за управление на сигурността на информацията, съгласно изискванията на стандарт ISO/IEC 27001:2013, разширен до ISO 27701:2019, ISO/IEC 27017:2015, ISO/IEC 27018:2019 до м. октомври 2024

3. Провеждане на втори надзорен одит и преход към изискванията ISO/IEC 27001:2022 на Системата за управление на сигурността на информацията и съответно надзорен одит спрямо изискванията на стандартите ISO 27701:2019, ISO/IEC 27017:2015, ISO/IEC 27018:2019. Крайният срок на провеждане на одита и издаване на сертификат след взето сертификационно решение трябва да бъде в съответствие с изискванията на IAF MD 26:2022 г., но не по-късно от 25 октомври 2025 г.

4. Издаване на сертификати за съответствие и предоставяне на лого на сертифициращата организация

4.1. След ресертификационния одит през 2023 по стандарт ISO/IEC 27001:2013 на български и на английски език. Предоставяне за ползване на лого (сертификационен символ, представляващ лого на Органа по сертификация и съответния стандарт – версия ISO/IEC 27001:2013)

4.2. След втори надзорен одит през 2025 г. и преход към изискванията на стандарта ISO/IEC 27001:2022 се очаква преиздаване на сертификатите на Системата за управление на сигурността на информацията с валидност, отговаряща на спазените изисквания IAF MD 26:2022 г. за добавяне на допълнително време към надзорния одит. След издаване на новите сертификати се предоставя за ползване лого (сертификационен символ, представляващ лого на Органа по сертификация и съответния стандарт – версия ISO/IEC 27001:2022)

II. ОБХВАТ И МЕСТОПОЛОЖЕНИЕ НА ПЛОЩАДКИТЕ В СИСТЕМАТА:

1. Обхват на сертификация (ресертификация):

Управление на информационната сигурност за защита на личните данни и задължения по договори, в обхвата на:

1. Приемане на съобщения, подадени във физическа или електронна форма от подателя, предаването им чрез далекосъобщителни средства и доставяне на тези съобщения на получателя като пощенски пратки (хибридна поща);

2. Пощенски марки и филателни продукти, полиграфически продукти и услуги;

3. Финансово посредничество, в това число парични преводи.

2. Брой служители/брой смени: 144/1;

3. Брой площадки: 7;

4. Адрес на площадките на „Български пощи" ЕАД :

4.1. Централно управление гр. София 1700, ул. „Академик Стефан Младенов", № 1, бл. 31;

4.2. Специализирано поделение „Българска филателия и нумизматика" гр.София 1612, ул. „Хайдушка поляна" № 8;

4.3. Регионално управление „Западен регион" гр. София 1700, ул. „Академик Стефан Младенов", № 1, бл. 31;

4.4. Регионално управление „Южен централен регион" гр. Пловдив 4000, пл. „Централен" № 1;

4.5. Регионално управление „Югоизточен регион" гр. Бургас 8000, ул. „Цар Петър" № 2;

4.6. Регионално управление „Североизточен регион" гр. Варна 9000, бул. „Съборни" № 42;

4.7. Регионално управление „Северен централен регион" гр. Плевен 5800, ул. „Хан Крум" № 3.

Числеността и класификацията на персонала по площадките на Системата, са посочени в Приложение № 1 към техническата спецификация.

III. СПЕЦИФИЧНИ ОБСТОЯТЕЛСТВА ПРИ ИЗВЪРШВАНЕТО НА ОДИТИ ОТ ТРЕТА СТРАНА НА ИНФОРМАЦИОННАТА СИСТЕМА И НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА.

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).

1.1. 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.

1.2.Прилага се изискването на ISO/IEC 27006:2015, т. 8.4.1 Достъп до организационни записи, което гласи, че 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.

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:

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.

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).

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.

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

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.

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.

Приложение: Численост и класификация на персонала в площадките на Системата.

Приложение № 1

ЧИСЛЕНОСТ И КЛАСИФИКАЦИЯ НА ПЕРСОНАЛА В ПЛОЩАДКИТЕ

Централно управление, София			
Персонал в обхвата на ISO/IEC 27001 Класификация на персонала	Пълно работно време .	Непълно работно време	Общо
Ръководство:			
Главен изпълнителен директор	1		1
Асистент на директора	1		1
Зам. изпълнителен директор	1		1
Директори на дирекции	8		8
Асистенти на директори на дирекции	8		8
Ръководители на отдели	16		16
Ръководители отдели на пряко подчинение на ГИД	3		3
Човешки ресурси	1		1
Финанси и икономика/счетоводство	1		1
Правна дейност	2		2
ДЛЗД	1		1
Връзки с обществеността	1		1
Call center /Кол център/	1		1
Работа Home office	0		0
ИКТ	6		6
Сигурност	4		4
Сигурност с ИРМ в БРСЦ	2		2
Служители на граждански договори	1		1
Общо			58

Специализирано поделение „Българска Филателия и Нумизматика", София			
Персонал в обхвата на ISO/IEC 27001 Класификация на персонала	Пълно работно време	Непълно работно време	Общо
Ръководство:			
Директор	1		1
Асистент на директора	1		1
Ръководител направление, в т.ч. Човешки ресурси	3		3
Главен технолог	1		1
Началник цех	4		4
Счетоводители	3		3
Правна дейност	1		1
БЗР	1		1
ТРЗ	1		1
Финансов контрол	1		1
Работа Home office	0		0
Служители от ЦУ с изнесено работно място: -ИКТ -Сигурност	1		1

Командировани от други организации	0		0
Служители на граждански договори	0		0
Общо			18

РУ „Западен регион“ - София			
Персонал в обхвата на ISO/IEC 27001 Класификация на персонала	Пълно работно време	Непълно работно време	Общо
Ръководство:			
Директор	1		1
Асистент на директора	1		1
Ръководител направление (ОУЛ/ФИ/ЧР)	3		3
Ръководител отдел/гл. експерт в направление ОУЛ	2		2
Счетоводител	1		1
Правна дейност	1		1
БЗР	1		1
Финансов контрол	1		1
Работа Home office	0		0
Командировани от други организации	0		0
Служители на граждански договори	0		0
Общо			11

РУ „Южен централен регион”- Пловдив,			
Персонал в обхвата на ISO/IEC 27001 Класификация на персонала	Пълно работно време	Непълно работно време	Общо
Ръководство:			
Директор	1		1
Асистент на директора	1		1
Ръководител направление (ОУЛ/ФИ/ЧР)	3		3
Ръководител отдел/гл. експерт в направление ОУЛ	2		2
Счетоводител	1		1
Правна дейност	1		1
БЗР	1		1
Финансов контрол	1		1
Работа Home office	0		0
Служители от ЦУ с изнесено работно място: -ИКТ -Сигурност	 1 1		 1 1
Командировани от други организации	0		0
Служители на граждански договори	0		0
Общо			13

РУ „Югоизточен регион"- Бургас			
Персонал в обхвата на ISO/IEC 27001 Класификация на персонала	Пълно работно време	Непълно работно време	Общо
Ръководство:			
Директор	1		1
Асистент на директора	1		1
Ръководител направление (ОУЛ/ФИ/ЧР)	3		3
Ръководител отдел/гл. експерт в направление ОУЛ	2		2
Счетоводител	1		1
Правна дейност	1		1
БЗР	1		1
Финансов контрол	1		1
Работа Home office	0		0
Служители от ЦУ с изнесено работно място: -ИКТ -Сигурност	 4 1		 4 1
Командировани от други организации	0		0
Служители на граждански договори	0		0
Общо			16

РУ „Североизточен регион" - Варна,			
Персонал в обхвата на ISO/IEC 27001 Класификация на персонала	Пълно работно време	Непълно работно време	Общо
Ръководство:			
Директор	1		1
Асистент на директора	1		1
Ръководител направление (ОУЛ/ФИ/ЧР)	3		3
Ръководител отдел/гл. експерт в направление ОУЛ	2		2
Счетоводител	1		1
Правна дейност	1		1
БЗР	1		1
Финансов контрол	1		1
Работа Home office	0		0
Служители от ЦУ с изнесено работно място: -ИКТ -Сигурност	 3 1		 3 1
Командировани от други организации	0		0
Служители на граждански договори	0		0
Общо			15

РУ „Северен централен регион" - Плевен			
Персонал в обхвата на ISO/IEC 27001 Класификация на персонала	Пълно работно време	Непълно работно време	Общо
Ръководство:			
Директор	1		1
Асистент на директора	1		1
Ръководител направление (ОУЛ/ФИ/ЧР)	3		3
Ръководител отдел/гл. експерт в направление ОУЛ	2		2
Счетоводител	1		1
Правна дейност	1		1
БЗР	1		1
Финансов контрол	1		1
Работа Home office	0		0
Служители от ЦУ с изнесено работно място: -ИКТ -Сигурност	 1 1		 1 1
Командировани служители	0		0
Служители на граждански договори	0		0
Общо			13