Д О Г О В О Р

№ .....

В гр. София, между:

1. МИНИСТЕРСТВОТО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ, ЕИК 180680495 с адрес: гр. София 1000, ул. „Ген. Гурко“ № 6, представлявано от Валентин Мундров – министър на електронното управление и – директор на дирекция „Финанси“, в качеството на ВЪЗЛОЖИТЕЛ и БЕНЕФИЦИЕР, наричано по-долу за краткост ВЪЗЛОЖИТЕЛ

и

2. „ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД, ЕИК 831641791, със седалище и адрес на управление: гр. София 1504, район Оборище, ул. „Панайот Волов“ № 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството и - главен счетоводител, наричано по-долу за краткост ИЗПЪЛНИТЕЛ, от друга страна,

двете наричани по-долу за краткост „страни“, като взеха предвид че:

- услугите, предмет на настоящия договор, представляват дейности по системна интеграция, по смисъла на чл. 7с от ЗЕУ;
- съгласно § 45, ал. 1, изр. 1-во от ПЗР към ЗИД на ЗЕУ системната интеграция по чл. 7с от ЗЕУ, в която са включени услуги по изграждане, поддържане, развитие и наблюдение на работоспособността на информационните и комуникационните системи, използвани от административните органи, както и дейности, които осигуряват изпълнението на тези услуги, се извършва от „Информационно обслужване“ АД, в качеството му на публичен възложител;
- на основание § 45, ал. 2 от ПЗР към ЗИД на ЗЕУ съгласно т. 30 от Решение № 727 на Министерския съвет от 2019 г., с последващи изменения и допълнения ВЪЗЛОЖИТЕЛЯТ е определен като административен орган, който при изпълнение на своите функции, свързани с дейности по системна интеграция, възлага изпълнението на тези дейности на системния интегратор „Информационно обслужване“ АД;

- ВЪЗЛОЖИТЕЛЯТ е контролиращ орган на ИЗПЪЛНИТЕЛЯ по смисъла на чл. 12, Параграф 1 от Директива 2014/24/ЕС.

- Съгласно чл.7г от ЗЕУ Министърът на електронното управление упражнява върху всички административни органи контрол в рамките на бюджетния процес по отношение на разходите в областта на електронното управление и за използваните от тях информационни и комуникационни технологии и разполага с правомощието да издава задължителни

разпореждания до административните органи и лицата по чл. 1, ал. 2 относно спазването на изискванията на ЗЕУ (чл. 7и ЗЕУ),

сключиха настоящия Договор („Договора/Договорът“), с който се споразумяха за следното:

I. ПРЕДМЕТ НА ДОГОВОРА И МЯСТО НА ИЗПЪЛНЕНИЕ

Чл. 1. (1) ВЪЗЛОЖИТЕЛЯТ възлага, а ИЗПЪЛНИТЕЛЯТ приема да предостави на ВЪЗЛОЖИТЕЛЯ услуги по системна интеграция, попадащи в обхвата на чл. 7с от ЗЕУ, съгласно заложеното в Техническите параметри (Приложение № 1), неразделна част от настоящия договор.

(2) В обхвата на договора се включват следните дейности[1]:

1. Предоставяне на услуги по управление и наблюдение на киберсигурността на информационно-комуникационната инфраструктура (ИКИ) на Министерство на електронното управление (МЕУ) и ИАИЕУ.

2. Оперативно управление, наблюдение, ескалация, оперативна координация и реакция при инциденти на административни органи в Република България.

3. Управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ) на МЕУ и ИАИЕУ в направление автентикация, оторизация, организация на база данни от потребители и компютри.

(3) ИЗПЪЛНИТЕЛЯТ се задължава да осигури изпълнението на дейностите по договора в съответствие с изискванията на Техническите параметри, неразделна част от настоящия договор.

Чл. 2. (1) Място на изпълнение на дейностите по договора: Центърът за киберсигурност на „Информационно обслужване“ АД

(2) При необходимост, по време на изпълнение на дейностите в обхвата на договора е възможно дейности, които не са свързани с достъп до информация, представляваща служебна тайна, да бъдат извършвани на място, различно от посоченото в ал. 1.

(3) При промяна на оборудването, обект на наблюдение, или необходимост от включване на допълнителни дейности в обхвата на услугата, условията за това ще бъдат предмет на допълнителни споразумения, неразделна част от настоящия договор.

[1] Посочват се основните дейности, включени в Техническите параметри.

II. СРОК НА ДЕЙСТВИЕ И ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ

Чл. 3. (1) Договорът влиза в сила от датата на подписването му от страните и е със срок на действие до приемане на изпълнение на всички задължения на страните по договора.

(2) ИЗПЪЛНИТЕЛЯТ се задължава да изпълнява дейностите по чл. 1, ал. 2 в периода от 15.08.2025 г. до 14.08.2028 г. включително. [2]

(3) При възникване на непредвидени обстоятелства, вкл. обжалване на решения на ВЪЗЛОЖИТЕЛЯ или на ИЗПЪЛНИТЕЛЯ, посоченият/те в ал. 1 срокове се считат за автоматично продължен/и със срока на действие на съответните непредвидени обстоятелства, за което се изготвя констативен протокол. Констативният протокол се съставя като електронен документ и се подписва от лицата по чл. 18 и чл. 19 от Договора с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис.

Чл. 4. (1) Договорът се прекратява:

1. С изтичане на срока на Договора и изпълнение на всички задължения на страните;

2. По взаимно съгласие на страните, изразено в писмена форма;

3. При настъпване на обективна невъзможност за изпълнение на договора, както и при отмяна на правата на системния интегратор за изпълнение на съответните дейности, посредством промяна в нормативната уредба. За избягване на съмнение случаите на изменение на правната уредба включват и приемането на акт от правителството на Република България, който може да уреди по друг начин възлагането на дейността по системна интеграция на настоящия системен интегратор.

(2) В случай, че ИЗПЪЛНИТЕЛЯТ наруши съществено условие на настоящия Договор, и не успее да отстрани нарушението в срок до 30 (тридесет) дни от писмено уведомление за извършеното нарушение, ИЗПЪЛНИТЕЛЯТ е в неизпълнение и ВЪЗЛОЖИТЕЛЯТ има право да развали Договора без предизвестие. При настъпването на всяко „нарушаване на съществено условие по Договора“ от страна на ИЗПЪЛНИТЕЛЯ, се съставя протокол, подписан от лицата по чл. 18 и чл. 19, определени от страните по Договора за отговарящи за изпълнението му. За „съществено условие” по смисъла на изречение първо се счита такова условие, което е свързано с основните права и задължения на страните по Договора, и чието неизпълнение води до неизпълнение на предмета на Договора.

(3) ВЪЗЛОЖИТЕЛЯТ може по своя преценка да удължи 30-дневния период по ал. 2 за такъв период, за който ИЗПЪЛНИТЕЛЯТ продължава нормалните усилия за отстраняване на неизпълнението.

[2] Посочва се общият срок, както и срокове за изпълнение на отделни дейности/ отделни етапи на изпълнение на дейности (когато е приложимо)-

(4) ВЪЗЛОЖИТЕЛЯТ има право едностранно да прекрати договора:

1. при започване на процедура по ликвидация на ИЗПЪЛНИТЕЛЯ;

2. при откриване на производство за обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ, както и при обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ;

(5) При прекратяване на Договора, ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ всички суми за дейностите, изпълнени съгласно този Договор, които са били дължими към момента на прекратяването му.

(6) Независимо от основанието за прекратяване, всяко право на ползване (лиценз) на софтуерни продукти и/или поддръжка на лиценз, осигурени и приети от ВЪЗЛОЖИТЕЛЯ в изпълнение на настоящия Договор, запазва своето действие до изтичане на срока, за който са осигурени.

III. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 5. (1) За изпълнение на възложените дейности, съгласно предмета на договора по чл. 1. ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ възнаграждение („обща цена“ или „общо възнаграждение“ в размер на 5 760 000.00 (пет милиона седемстотин и шестдесет хиляди) лева без ДДС, или 2 945 041.24 EUR (два милиона деветстотин четиридесет и пет хиляди и четиридесет и едно евро и двадесет и четири евро цента) без ДДС, съответно 6 912 000.00 (шест милиона деветстотин и дванадесет хиляди) лева с ДДС или 3 534 049.49 EUR (три милиона петстотин тридесет и четири хиляди и четиридесет и девет евро и четиридесет и девет евро цента) с ДДС при действаща 20 % ставка на ДДС, платими на равни тримесечни вноски в размер на 480 000.00 лв. без ДДС или 245 420.10 EUR без ДДС.

(2) В Цената по ал. 1 са включени всички разходи на ИЗПЪЛНИТЕЛЯ за изпълнение на Услугите, като ВЪЗЛОЖИТЕЛЯТ не дължи заплащането на каквито и да е други разноски, направени от ИЗПЪЛНИТЕЛЯ. При законодателна промяна в размера на приложимата ставка, възнаграждението се актуализира в съответствие с настъпилото изменение, с подписване на допълнително споразумение.

(3) Цената по ал. 1 включва изпълнение на дейностите, посочени в Приложение № 1 към договора.

(4) ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ цената за извършената услуга/ цената на съответната изпълнена дейност[3], предмет на този договор, за съответния отчетен период в срок до 30 (тридесет) дни от получаване на издадена от ИЗПЪЛНИТЕЛЯ оригинална

[3]Когато предметът на договора включва повече от една дейност/ етапи на изпълнение на дейности и всяка отделна дейност и/или етап на изпълнение на дейност има цена.

фактура и подписани между ИЗПЪЛНИТЕЛЯ и ВЪЗЛОЖИТЕЛЯ двустранни приемо-предавателни протоколи (за приемането на резултатите от изпълнението на дейностите по чл. 1, ал. 2 от договора) от ръководителите на договора за двете страни, при спазване на условията по ал. 5.

(5) Плащането/плащанията по този Договор се извършва/т въз основа на следните документи:

1. двустранни приемо-предавателни протоколи (за приемането на резултатите от изпълнението на дейностите/ етапи на изпълнение на дейности по чл. 1, ал. 2 от договора), съставени като електронни документи и подписани от ръководителите на договора за ИЗПЪЛНИТЕЛЯ и ВЪЗЛОЖИТЕЛЯ с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯ, придружени от съответните документи - резултати от изпълнението на дейностите по чл. 1, ал. 2 от договора в съответствие с изискванията на Техническите параметри, които са неразделна част от настоящия договор и при съответно спазване на разпоредбите на Раздел VII (Отговорности) от Договора; и

2. фактура, издадена от ИЗПЪЛНИТЕЛЯ, представена на ВЪЗЛОЖИТЕЛЯ и подписана от ръководителя по договора за ВЪЗЛОЖИТЕЛЯ.

(6) Допуска се цената по ал.1 да се заплаща:

1. чрез акредитив, при условия съгласувани между ИЗПЪЛНИТЕЛЯ и ВЪЗЛОЖИТЕЛЯ. Таксите и комисионните за обслужване на акредитивната сметка се заплащат както следва: 50 % от ИЗПЪЛНИТЕЛЯ и 50% от ВЪЗЛОЖИТЕЛЯ;

2. авансово - след представяне от страна на ИЗПЪЛНИТЕЛЯ на гаранция, която обезпечава авансово предоставените средства. На основание чл. 113, ал. 4 от Закона за данък върху добавената стойност, ИЗПЪЛНИТЕЛЯТ издава фактура за авансовото плащане не по-късно от 5 дни от датата на получаване на плащането и я предоставя на ВЪЗЛОЖИТЕЛЯ .

(7) Преди извършване на плащане от ВЪЗЛОЖИТЕЛЯ се прилагат правилата на Министерство на финансите за извършване на плащания от разпоредители с бюджет.

Чл. 6. (1) Изплащането на договореното възнаграждение, в размер, определен съгласно чл. 5, ал. 1 се извършва по следната банкова сметка на ИЗПЪЛНИТЕЛЯ:

Банка:

BIC:

IBAN:

Заличаването на IBAN на Изпълнителя е на основание чл. 72 и чл. 73 от ДОПК.

(2) При промяна на банковата сметка, посочена от ИЗПЪЛНИТЕЛЯ, преди извършване на дължимото плащане, същият уведомява ВЪЗЛОЖИТЕЛЯ писмено в 3-дневен срок от

настъпване на промяната. В случай, че не уведоми ВЪЗЛОЖИТЕЛЯ в този срок, плащането по посочената в Договора сметка се счита за валидно извършено.

Чл. 7. Страните се съгласяват, че в случай, че съответната коректно издадена фактура не е получена от ВЪЗЛОЖИТЕЛЯ, няма да е налице забава от страна на ВЪЗЛОЖИТЕЛЯ за плащане на дължимите суми и не се дължи лихва за забава за периода, с който е забавено представянето на фактурата.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

Чл. 8. ИЗПЪЛНИТЕЛЯТ се задължава да изпълни дейностите, предмет на договора, съгласно чл. 1 от същия, при спазване на изискванията, посочени в Техническите параметри – Приложение № 1 към същия.

Чл. 9. (1) ИЗПЪЛНИТЕЛЯТ се задължава да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 20 от Договора. Да опазва и да не разгласява пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена по закон или по силата на Договора информация, която е станала известна при изпълнението на дейностите по чл. 1, ал. 2, като представи декларация по образец – Приложение №2.

(2) При изпълнение на предмета на Договора, посочен в чл. 1, ИЗПЪЛНИТЕЛЯТ се задължава да прилага някои или всички изброени по-долу изисквания, съобразно обхвата на възложената дейност:

а) да спазва изискванията на действащата нормативна уредба в областта на мрежовата и информационната сигурност;

б) да прилага адекватни мерки за мрежова и информационна сигурност, включително да доказва прилагането им чрез документи и/или провеждане на одити при необходимост;

в) да прилага система за прозрачност на веригата на доставките, като при поискване, трябва да може да докаже произхода на предлагания ресурс/ услуга и неговата сигурност;

(3) При възлагане изпълнението на дейностите на трети лица, ИЗПЪЛНИТЕЛЯТ следва да изисква от същите да прилагат всички, изброени в ал. 2, изисквания, съобразно обхвата на възложената дейност.

Чл. 10 (1) При изпълнение на дейностите по договора ИЗПЪЛНИТЕЛЯТ, неговите подизпълнители и служители се задължават:

1. да спазват политиката, правилата и процедурите по информационна сигурност на ВЪЗЛОЖИТЕЛЯ;
2. да опазват и да не разгласяват пред трети лица съдържанието на документацията,

която е станала известна при изпълнението на този договор, без писменото съгласие на ВЪЗЛОЖИТЕЛЯ, с изключение на случаите, когато са задължени по закон за това;

3. да опазват и да не разгласяват пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор;

4. да обработва законосъобразно и добросъвестно лични данни, доколкото тези данни са изрично необходими за целите на изпълнение на поетия ангажимент;

5. да предоставя лични данни на публични органи (държавни и общински), когато такива данни са изискани въз основа на валидно законово основание и по законоустановен за целта ред, като своевременно уведоми за това ВЪЗЛОЖИТЕЛЯ;

6. да предприеме всички необходими организационни и технически мерки за осигуряване на целостта и поверителността на данните в случай, че ВЪЗЛОЖИТЕЛЯТ предостави на ИЗПЪЛНИТЕЛЯ достъп до собствени IT активи, документи и данни;

7. да опазват и да не разгласяват пред трети лица информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, както и да не разгласяват, използват или предоставят на трети лица разработена в полза на ВЪЗЛОЖИТЕЛЯ или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор, с изключение на случаите, когато са задължени по закон за това;

8. да спазват вътрешните правила за достъп и режим на работа в сградата/ сградите на ВЪЗЛОЖИТЕЛЯ;

9. да спазват всички процедури и изисквания на ВЪЗЛОЖИТЕЛЯ за работа в информационната инфраструктура на ВЪЗЛОЖИТЕЛЯ;

10. да не осъществяват достъп до компютърни данни в компютърна система без разрешение, да не добавят, променят, изтриват или унищожават компютърна програма или компютърни данни, да не въвеждат компютърен вирус в компютърните системи или мрежи на ВЪЗЛОЖИТЕЛЯ, да не разпространяват пароли или кодове за достъп до компютърна система или до компютърни данни на ВЪЗЛОЖИТЕЛЯ, от което би могло да последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна;

(2) С оглед изпълнението на задълженията по ал. 1, ИЗПЪЛНИТЕЛЯТ (представляващите го лица), както и лицата, ангажирани с изпълнението на дейностите (екипа на ИЗПЪЛНИТЕЛЯ), представят декларация за опазване на информацията.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ

Чл. 11. (1) ВЪЗЛОЖИТЕЛЯТ следва да предоставя на ИЗПЪЛНИТЕЛЯ необходимото съдействие за изпълнение на Договора.

(2) ВЪЗЛОЖИТЕЛЯТ е длъжен да приеме и заплати извършеното от ИЗПЪЛНИТЕЛЯ в съответствие с Договора.

(3) За постигането на резултатите по дейностите, ВЪЗЛОЖИТЕЛЯТ, чрез неговия екип, се задължава да предостави информация за: изградената при ВЪЗЛОЖИТЕЛЯ ИТ архитектура и свързаност на системите, касаещи предмета на договора.

(4) При необходимост, ВЪЗЛОЖИТЕЛЯТ ще осигури условия за провеждане на работни срещи за изпълнението на договора. Местата ще бъдат осигурени на ангажираните от ИЗПЪЛНИТЕЛЯ лица, при съблюдаване на изискванията на Закона за здравословни и безопасни условия на труд (ЗБУТ).

(5) ВЪЗЛОЖИТЕЛЯТ се задължава да осигури на ИЗПЪЛНИТЕЛЯ, достъп до сградата на ВЪЗЛОЖИТЕЛЯ, съгласно вътрешните процедури на ВЪЗЛОЖИТЕЛЯ за осигуряване на достъп, за целите на изпълнение на дейностите по договора.

(6) ВЪЗЛОЖИТЕЛЯТ се задължава да предостави достъп до необходимите за изпълнение на дейностите по договора ИТ активи, документация и данни, при получаване на обосновано искане от ИЗПЪЛНИТЕЛЯ.

(7) За ВЪЗЛОЖИТЕЛЯ няма задължение за осигуряване на офис-техника, консумативи и др. Цялото необходимо оборудване, вкл. техническо, програмно и друго за целите на работата на екипа на ИЗПЪЛНИТЕЛЯ, следва да бъде осигурено от него. За целите на извършване на работата по Техническите параметри, ВЪЗЛОЖИТЕЛЯТ се задължава да предостави достъп на ИЗПЪЛНИТЕЛЯ до онази информация, приложения и технологична среда, която е необходима за успешното извършване на работата и при спазване на утвърдените процедури, правила и политики на ВЪЗЛОЖИТЕЛЯ.

VI. ОБЩИ И СПЕЦИАЛНИ УСЛОВИЯ ПО ЗЗБУТ

Чл. 12 (1) В случаите на осигуряване на работни места, ВЪЗЛОЖИТЕЛЯТ и ИЗПЪЛНИТЕЛЯТ се задължават да осигурят прилагането на правила за съвместно осигуряване на здравословни и безопасни условия на труд за административните сгради, с адрес: гр. София, ул. Лъчезар Станчев, № 11 в изпълнение на разпоредбата на чл. 18 от ЗЗБУТ, както следва:

1. определят задълженията и отговорностите си за осигуряване на здравословни и безопасни условия на труд при работа на работниците и служителите, както и здравословни и безопасни условия за други лица, които се намират в района на мястото на извършване на дейностите по договора;

2. информират своевременно за възможните опасности и рисковете при работа съгласно ЗЗБУТ и действащите вътрешни правила;

3. координират дейностите си за предпазване на работниците и служителите от тези рискове;

4. прилагат всички нормативни документи, отнасящи се до спазване на изискванията за ЗБУТ.

(2) С възлагане на дейността, ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯТ, следва да поемат следните конкретни задължения за осигуряване на ЗБУТ:

1. На служителите на ИЗПЪЛНИТЕЛЯ се провежда начален и периодични инструктажи от длъжностните лица, определени за това, съгласно изискванията на Наредба № РД-07-2/2009 г. за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд;

2. ВЪЗЛОЖИТЕЛЯТ следва да запознае служителите на ИЗПЪЛНИТЕЛЯ с разработения, съгласно Наредба № 8121з-647/2014 г. за правилата и нормите за пожарна безопасност при експлоатация на обектите, план за пожарна и аварийна безопасност, план за евакуация, схеми за евакуация с обозначение на евакуационните изходи и средствата за пожарогасене и да извърши обучение за евакуация и работа с пожарогасителна техника;

3. ВЪЗЛОЖИТЕЛЯТ предоставя на служителите на ИЗПЪЛНИТЕЛЯ информация за рисковете за здравето и безопасността на неговите служители, както и за мерките, които се предприемат за отстраняването, намаляването или контролирането им, при необходимост.

4. Всички останали изисквания по време на изпълнение на дейностите, извън посочените в настоящия документ ангажименти на ВЪЗЛОЖИТЕЛЯ по отношение на работна среда и условията за работа, ще бъдат допълнително уточнени, след получаване на заявка от страна на ИЗПЪЛНИТЕЛЯ, ведно с обосновка на необходимостта за тяхното предоставяне и съгласно възможността от страна на ВЪЗЛОЖИТЕЛЯ за това.

(3) При необходимост, ВЪЗЛОЖИТЕЛЯ се задължава да осигури:

1. ползване на стационарни телефони с вътрешна и външна линия, като разговорите се заплащат от ИЗПЪЛНИТЕЛЯ въз основа на издадена фактура от ВЪЗЛОЖИТЕЛЯ;

2. условия за провеждане на работни срещи.

VII. ОТГОВОРНОСТИ

Чл. 13. (1) При пълно виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи на ВЪЗЛОЖИТЕЛЯ неустойка в размер на 5 % от общото възнаграждение по чл. 5, ал. 1 без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 30-дневен срок от уведомяването. За пълно неизпълнение се приема неизвършването на нито една от дейностите, включени в обхвата на договора по чл. 1, ал. 2.

(2) При частично виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи на ВЪЗЛОЖИТЕЛЯ неустойка в размер на 1 % от общото възнаграждение[4] / 5 % от възнаграждението за съответната дейност/ за етап от дейност [5] по чл. 5, ал. 1 на договора без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 30-дневен срок от уведомяването. За частично неизпълнение се приема неизвършването на дейност, включена в обхвата на договора по чл. 1, ал. 2.

(3) В случай, че ИЗПЪЛНИТЕЛЯТ е в забава по негова вина, ВЪЗЛОЖИТЕЛЯТ има право да получи неустойка за забавено изпълнение в размер на 0,01 % на ден върху общото възнаграждение[6] по чл. 5, ал. 1 на договора без ДДС / 0,05 % на ден от възнаграждението за съответната дейност/ за етап от дейност[7] по чл. 5, ал. 1 на договора без ДДС, считано от деня, следващ деня, в който ИЗПЪЛНИТЕЛЯТ е следвало да извърши съответната дейност, но не повече от 1% от общото възнаграждение по чл. 5, ал. 1 без ДДС.

(4) В случай че е налице забава по вина на ВЪЗЛОЖИТЕЛЯ, ИЗПЪЛНИТЕЛЯТ не дължи неустойка за забавено изпълнение.

(5) При констатирано лошо или друго неточно или частично изпълнение или при отклонение от изискванията на ВЪЗЛОЖИТЕЛЯ, същият има право да поиска от ИЗПЪЛНИТЕЛЯ да изпълни дейността изцяло и качествено, без да дължи допълнително възнаграждение за това. В случай, че и повторното изпълнение на дейността е некачествено, ВЪЗЛОЖИТЕЛЯТ има право да изиска неустойка в размер на 2 % от общото възнаграждение по чл. 5, ал. 1 без ДДС[8] / 4 % от възнаграждението за съответната дейност/ за етап от дейност [9] по чл. 5, ал. 1 на договора без ДДС.

---

[4] Приложимо е в случаите, когато в чл.5, ал.1 е уговорена само обща цена-

[5] Приложимо е когато предметът на договора включва повече от една дейност/ етапи на изпълнение на дейности и всяка отделна дейност и/или етап на изпълнение на дейност има цена.

[6] Приложимо е в случаите, когато в чл.5, ал.1 е уговорена само обща цена-

[7] Приложимо е когато предметът на договора включва повече от една дейност/ етапи на изпълнение на дейности и всяка отделна дейност и/или етап на изпълнение на дейност има цена.

[8] Приложимо е в случаите, когато в чл.5, ал.1 е уговорена само обща цена

[9] Приложимо е когато предметът на договора включва повече от една дейност/ етапи на изпълнение на

(6) Всяка забава се удостоверява с констативен протокол, подписан от ВЪЗЛОЖИТЕЛЯ и от ИЗПЪЛНИТЕЛЯ, чрез лицата по чл. 18 и чл. 19.

(7) ВЪЗЛОЖИТЕЛЯТ може да претендира обезщетение за нанесени вреди и/или пропуснати ползи по общия ред, независимо от начислените неустойки, включително при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност.

(8) При забава в плащане на уговореното възнаграждение ВЪЗЛОЖИТЕЛЯТ дължи на ИЗПЪЛНИТЕЛЯ обезщетение в размер на 0,05% на ден върху размера на съответното забавено плащане без ДДС, но не повече от 5% от стойността на забавеното плащане без ДДС.

Чл. 14. Страните запазват правото си да търсят обезщетение за вреди, ако тяхната стойност е по-голяма от изплатените неустойки по реда на този раздел.

VIII. АВТОРСКИ ПРАВА

Чл. 15. (1) Авторските и всички сродни права и собствеността върху изработени софтуерни продукти, техният изходен програмен код, дизайнът на интерфейсите и базите данни, чиято разработка попада в обхвата на чл. 1, ал. 1 от договора и всички съпътстващи изработката им проучвания, разработки, скици, чертежи, планове, модели, документи, софтуер, дизайни, описания, документи, данни, файлове, матрици или каквито и да било средства и носители и свързаната с тях документация и други продукти, възникват директно за ВЪЗЛОЖИТЕЛЯ, в пълния им обем, съгласно действащото законодателство, а в случай че това не е възможно ще се считат за прехвърлени на ВЪЗЛОЖИТЕЛЯ в пълния им обем, без никакви ограничения в използването, изменението и разпространението им и без ВЪЗЛОЖИТЕЛЯТ да дължи каквито и да било допълнителни плащания и суми освен предвидената в договора стойност. ИЗПЪЛНИТЕЛЯТ потвърждава, че Техническите параметри и цялата информация предоставена му от ВЪЗЛОЖИТЕЛЯ за изпълнение на задълженията му по настоящия Договор, са изключителна собственост на ВЪЗЛОЖИТЕЛЯ и същият притежава авторските права върху тях, като ИЗПЪЛНИТЕЛЯТ/ третите лица, на които е възложено изпълнението единствено адаптират концепцията на ВЪЗЛОЖИТЕЛЯ във вид и по начин, позволяващи използването й за посочените по-горе цели, като всички адаптации, направени в изпълнение на този Договор, както и авторските права върху тях остават изключителна собственост на ВЪЗЛОЖИТЕЛЯ и могат да бъдат използвани по негово собствено усмотрение свободно в други проекти, развивани, или осъществявани от него.

дейности и всяка отделна дейност и/или етап на изпълнение на дейност има цена.

(2) При разработване на софтуер за ВЪЗЛОЖИТЕЛЯ, настоящият раздел от договора се счита и следва да бъде тълкуван като договор за създаване на обект на авторско право (произведение) по поръчка, съгласно чл. 42 ал. 1 от Закон за авторското право и сродните му права (ЗАПСП), като Страните изрично се съгласяват и споразумяват, че:

1. авторските права върху софтуерните продукти и части от тях, включително имуществените права съгласно раздел II от ЗАПСП и прехвърлимите неимуществени права, съгласно чл. 15 от ЗАПСП ще възникнат и принадлежат изцяло и безусловно на ВЪЗЛОЖИТЕЛЯ, като ИЗПЪЛНИТЕЛЯТ декларира и гарантира, че те няма да бъдат обременени с каквито и да било тежести, залози, искове, претенции на трети лица, възбрани и други тежести или права на трети лица;

2. ИЗПЪЛНИТЕЛЯТ предоставя на ВЪЗЛОЖИТЕЛЯ изключителни права по смисъла на чл. 36, ал. 2 от ЗАПСП за използване на Софтуерните продукти и техни елементи, и обектите, изброени в ал. 1 или части от тях, в случай че авторските права върху тях не могат да възникнат директно за ВЪЗЛОЖИТЕЛЯ.

(3) За избягване на съмнение, Страните потвърждават и се съгласяват, че правата на ВЪЗЛОЖИТЕЛЯ върху софтуерните продукти и обектите, изброени в ал. 1, включително и изключителното право на ползване по ал. 2, т. 2 обхващат всички видове използване, както е предвидено в ЗАПСП, без никакви ограничения по отношение на срокове и територия, включително, но не само: право на ползване, промяна, изменение, възпроизвеждане, публикуване, разпространение, продажба, адаптиране, прехвърляне, представяне, маркетинг, разпореждане по какъвто и да било начин и с каквито и да било средства в най-широк възможен смисъл и по най-широк възможен начин за целия срок на действие и закрила на авторското право, за всички държави, където това право може да бъде признато. Това право на ВЪЗЛОЖИТЕЛЯ е без ограничение по отношение на броя на възпроизвеждането, разпространението или представянето и е валидно за всички държави, езици и начин на опериране. Освен това ИЗПЪЛНИТЕЛЯТ потвърждава и се съгласява, че цялата търговска репутация и ползи, произтичащи от софтуерните продукти ще възникват и принадлежат на ВЪЗЛОЖИТЕЛЯ и ИЗПЪЛНИТЕЛЯТ няма да има каквито и да било права и/или претенции в това отношение. ИЗПЪЛНИТЕЛЯТ също потвърждава и се съгласява, че няма и не може да предявява претенции по отношение на каквито и да било права на интелектуална собственост върху Софтуерните продукти.

(4) С изброените по-горе задължения, ИЗПЪЛНИТЕЛЯТ следва да задължи и трети лица, на които ще възложи за изпълнение дейностите по настоящия договор да не прехвърлят на други лица каквито и да било права свързани със софтуерни продукти, включително, но не

само правото на ползване и/или на промяна, както и нямат право да използват и/или прехвърлят, разкриват или предоставят по какъвто и да било начин на други лица концепцията на ВЪЗЛОЖИТЕЛЯ, съдържаща се в предоставените Технически параметри или други документи, предоставени по повод изпълнението на договора.

IX. ДРУГИ УСЛОВИЯ

Чл. 16. Всички съобщения, уведомления и документи по изпълнението на настоящия договор се съставят в електронен вид и се подписват с електронен подпис в PDF -формат. Кореспонденцията се извършва чрез електронна поща на електронните адреси, посочени от страните.

Чл. 17. Спорни въпроси, възникнали при действието на този договор се решават по пътя на споразумения, а нерешените се отнасят за решаване от компетентния съд.

Чл. 18. Отговарящ за изпълнението на договора от страна на ВЪЗЛОЖИТЕЛЯ наричан ръководител договор за времето на неговото действие е , директор на дирекция „Мрежова информационна сигурност“, тел: , ел. адрес: , а в негово/нейно отсъствие , началник отдел „Стратегии и политики в киберсигурността“, тел: , ел.адрес:

Чл. 19. Отговарящ за изпълнението от страна на ИЗПЪЛНИТЕЛЯ, наричан ръководител договор за времето на неговото действие, е , Мениджър ИТ услуги, отдел Системна интеграция, тел: ; имейл: , а в негово отсъствие: , Координатор сигурност, отдел Киберзащита и управление на информационната сигурност тел: ; имейл:

Чл. 20. (1) Всяка от Страните по този Договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала ѝ известна при или по повод изпълнението на Договора („Конфиденциална информация“). Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и

да е естество или в каквато и да е форма, включително, финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни, образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство, свързани с изпълнението на Договора

(2) Конфиденциална информация за целите на настоящия договор включва и:

1. съдържанието на документацията, която е станала известна при изпълнението на договора;

2. съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на договора;

3. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, разработена в полза на ВЪЗЛОЖИТЕЛЯ или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящата поръчка.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на Договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и действащата нормативна уредба.

(4) С изключение на случаите, посочени в ал. 5 на този член, Конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата Страна, като това съгласие не може да бъде отказано безпричинно.

(5) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. информацията е станала или става публично достъпна, без нарушаване на този Договор от която и да е от Страните;

2. информацията се изисква по силата на закон, приложим спрямо която и да е от Страните; или

3. предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната Страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 Страната, която следва да предостави информацията, уведомява незабавно другата Страна по Договора.

(6) Задълженията по този член се отнасят до ИЗПЪЛНИТЕЛЯ, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, като ИЗПЪЛНИТЕЛЯТ отговаря за изпълнението на тези задължения от страна на такива лица.

(7) Задълженията, свързани с неразкриване на Конфиденциалната информация остават в сила и след прекратяване на Договора на каквото и да е основание.

(8) ИЗПЪЛНИТЕЛЯТ няма право да дава публични изявления и съобщения, да разкрива или разгласява каквато и да е информация, която е получил във връзка с извършване на дейностите, предмет на този договор, независимо дали е въз основа на данни и материали на ВЪЗЛОЖИТЕЛЯ или на резултати от работата на ИЗПЪЛНИТЕЛЯ, без предварителното писмено съгласие на ВЪЗЛОЖИТЕЛЯ, което съгласие няма да бъде безпричинно отказано или забавено.

X. НЕПРЕОДОЛИМА СИЛА

Чл. 21. (1) Страните не отговарят за неизпълнение на задължение по този Договор, когато невъзможността за изпълнение се дължи на непреодолима сила. За целите на този Договор, „непреодолима сила“ има значението на това понятие по смисъла на чл. 306, ал. 2 от Търговския закон.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата Страна в срок до 3 *(три)* дни от настъпване на непреодолимата сила. Към уведомлението се прилагат всички релевантни и/или нормативно установени доказателства за настъпването и естеството на непреодолимата сила, причинната връзка между това обстоятелство и невъзможността за изпълнение, и очакваното времетраене на неизпълнението.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира, като страните подписват протокол, в който удостоверяват началната дата на спиране. Засегнатата Страна е длъжна, след съгласуване с насрещната Страна, да продължи да изпълнява тази част от задълженията си, които не са възпрепятствани от непреодолимата сила.

(4) След отпадане на непреодолимата сила, засегнатата страна в срок до 3 *(три)* дни уведомява писмено другата страна, като прилага всички релевантни и/или нормативно

установени доказателства за отпадането й. Страните подписват протокол, с който удостоверяват датата, от която се възобновява изпълнението на задълженията.

(5) Не може да се позовава на непреодолима сила Страна:

1. която е била в забава или друго неизпълнение преди настъпването на непреодолима сила;

2. която не е информирала другата Страна за настъпването на непреодолима сила; или

3. чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на Договора.

(6) Липсата на парични средства не представлява непреодолима сила.

Настоящият договор е изготвен като електронен документ и влиза в сила след подписването му с квалифициран електронен подпис от представителите на страните, като приложенията са негова неразделна част.

Приложения:

1. Приложение № 1 – Технически параметри;
2. Приложение № 2 – Образец на декларация за опазване на информацията.

ЗА ВЪЗЛОЖИТЕЛЯ:

ВАЛЕНТИН МУНДРОВ
МИНИСТЪР НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

ЗА ИЗПЪЛНИТЕЛЯ:

ИВАЙЛО ФИЛИПОВ
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР
НА „ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

ДИРЕКТОР НА ДИРЕКЦИЯ „ФИНАНСИ“

ГЛАВЕН СЧЕТОВОДИТЕЛ

Приложение № 1

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за предоставяне на услуги по управление и наблюдение на киберсигурността на информационно-комуникационната инфраструктура на Министерство на електронното управление (МЕУ) и Изпълнителна агенция „Инфраструктура на електронното управление“ (ИА ИЕУ), оперативно управление, наблюдение, ескалация, оперативна координация и реакция при инциденти на административни органи в Република България , както и управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ) на МЕУ и ИАИЕУ в направление автентикация, оторизация, организация на база данни от потребители и компютри

1. Цел на документа

Настоящият документ цели да опише обхвата на услугите по управление, наблюдение и киберсигурност на информационно-комуникационната инфраструктура на МЕУ и ИА ИЕУ, управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ) в направление автентикация, оторизация, организация на база данни от потребители и компютри, както и наблюдението, ескалацията и реакцията при инциденти свързани с административните органи.

2. Услуги

Настоящият документ дефинира изискванията на Възложителя за предоставяне на услуги за управление, наблюдение и киберсигурност на ИКИ за нуждите на МЕУ и ИА ИЕУ, управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ) на МЕУ и ИАИЕУ, както и оперативно управление, наблюдение, ескалация и реакция при инциденти на административните органи в Република България.

2.1. Цел на услугата за управление и наблюдение на киберсигурността на ИКИ на МЕУ и ИАИЕУ в режим 24*7 – включително всички вътрешни ресурси и мрежи на МЕУ и ИАИЕУ, Държавния хибриден частен облак (ДХЧО), Защитения интернет възел (ЗИВ) и Единната електронна съобщителна мрежа на държавната администрация и за нуждите на националната сигурност (ЕЕСМ) в частта киберсигурност.

Чрез осигуряването на услугата ще се постигне:

- Изпълнение на изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС).
- Непрекъснато наблюдение на критичната информационна инфраструктура на МЕУ и ИА ИЕУ.
- Предприемане на своевременни мерки за намаляване на риска от заплахи чрез анализ на мрежовия трафик, логовете на критични ИТ

активи - мрежови устройства, операционни системи, бази данни, приложен софтуер и др.

- Своевременно подобряване на политики и правила, свързани с информационната сигурност в МЕУ и ИА ИЕУ чрез предоставяното от Услугата интегрирано управление на данните от различни ИТ източници.
- Своевременно идентифициране на подходящи мерки за актуализиране на специализирания приложен софтуер, използван от МЕУ и ИА ИЕУ, с цел минимизиране на потенциални заплахи.

Изисквания към предоставянето на Услугата:

- На МЕУ се предоставят експерти за управление на информация, свързана със сигурността и реакция при инцидент. Процесът е изграден на база световно приети практики с вградени и настроени механизми за управление на сигурността на информацията и събитията.

Услугата следва да осигури постоянен мониторинг на ИТ дейности, комуникационна и информационна инфраструктура, ИТ услуги и взаимодействия с външни фактори в съответствие с изискванията на НМИМИС като се:

- Осигури наблюдение на крайните работни точки, присъединяване на други журнални файлове (log) към Системата, както и присъединяване на нови системи с възможност за непрекъснат мониторинг и анализ, с оглед предприемане на ответни мерки в случай на инцидент. „Информационно обслужване“ АД (ИО АД, ИЗПЪЛНИТЕЛ) ще изпраща информация по e-mail за аларми, по които е нужна допълнителна проверка от системен администратор на МЕУ или ИАИЕУ до 4 часа след тяхното настъпване. При установяване на неуспешна атака или фалшиво-позитивна аларма, e-mail към МЕУ не е необходимо да се изпраща. При нужда от асистенция, екипът на ИО АД ще съдейства за отстраняването на заплахите и възстановяване на работоспособността на системите и услугите.
- Извърши анализ на наличните уязвимости във вътрешната ИТ инфраструктура и предоставят препоръки и проследяване на изпълнението им, както и оказване на методическа помощ при идентифициране на потенциални заплахи и набелязване на мерки в краткосрочен план.
- Извършва анализ на базата на събраната информация поне за шестмесечен период и се предложат решения за извършване на промени в ИТ инфраструктурата в дългосрочен план.
- Провеждат срещи със служители, на които се дискутират, анализират и планират действия и мерки срещу актуалните заплахи към ИТ инфраструктурата, както и се оценява ефективността на предприетите мерки, чрез повторен анализ и оценка на действията по отстраняване на заплахи за всеки отчетен период
- При поискване от страна на МЕУ преглеждат, коригират и допълват изискванията за сигурност, включени в технически параметри или технически спецификации в областта на информационните и комуникационните системи.

Услугата следва да предостави и дейности по непрекъснато подобрение на сигурността чрез:

- Мониторинг за наличността на ключови услуги и своевременно информиране на МЕУ и ИАИЕУ при наличие на атаки до 1 час от установяването им;
- Съобщаване на установени от Системата инциденти до 1 работен ден с конкретни препоръки за отстраняването им;
- Установяване на кореновата причина за наличието на инцидент, извършване на корелационен анализ и препоръки за отстраняване;
- Управление на инциденти свързани със сигурността.
- Извършване на последващ контрол, координирано с администратор на МЕУ и/или ИАИЕУ за отстранени инциденти.
- Идентифициране на засегнатите от заплахите услуги/активи и даване на препоръки за действия от страна на МЕУ и/или ИАИЕУ.
- Ежемесечна автоматизирана проверка за наличие на уязвимости в публично видимите услуги на МЕУ и ИАИЕУ и вътрешните мрежи за управление.
- Процес по отстраняване и проследяване на уязвимости.

2.2. Цел на услуга оперативно управление, наблюдение, ескалация, оперативна координация и реакция при инциденти на административни органи в Република България

Чрез услугата ще се предоставят оперативно управление, наблюдение, ескалация, оперативна координация и реакция при инциденти на административни органи в Република България, както и дейности по непрекъснато подобрение на сигурността в Република България чрез:

- Идентифициране на засегнатите от заплахите услуги/активи и даване на препоръки за действия от страна на МЕУ и/или ИА ИЕУ.
- Разширено изпълняване на различните нива от Tier 1 до Tier 3 в режим 24/7/365, в следните направления координирани с МЕУ (Дирекция МИС,) и детайлно описани (Приложение 2), за нуждите на подпомагане на секторния екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС) екип за публичната администрация към МЕУ по мониторинг, реакция и превенция, чрез оперативно изпълнение и подпомагане дейностите на СЕРИКС:
    - Security Analysis – анализ на различни елементи и фази от кибератаки (напр. анализ на malware и др.).Извършване на последващ контрол, координирано с ЕЦК на МЕУ и/или ИА ИЕУ за отстранени инциденти при необходимост. Анализът е на база получен артефакт независимо от административната единица.
    - Vulnerability Management and Patch Management – Ежемесечна автоматизирана проверка за наличие на уязвимости в публично видимите услуги на публичната администрация, проактивно

откриване на повърхности на атака и последващо изготвяне на план и препоръки за тяхното смекчаване.

- Threat Hunting – проактивно търсене на компрометирани системи и услуги с цел ранно откриване на инциденти в публичната администрация.
- Threat Intelligence – мониторинг на киберобстановката в Република България относно хакерски групи, изтекли данни и акаунти, нови техники и тактики на атака и изграждане на threat profile за различните сектори и национално ниво.
- Incident Response and Handling – откриване на кибератаки и възстановяване от инциденти за всички административни единици в публичната администрация. Съобщаване на установени инциденти до 1 работен ден с конкретни препоръки за отстраняването им. Установяване на кореновата причина за наличието на инцидент, извършване на корелационен анализ и препоръки за отстраняване.

2.3 Цел на услуга по управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ) на МЕУ и ИАИЕУ в направление автентикация, оторизация, организация на база данни от потребители и компютри

Дейността по управление и наблюдение на ИКИ на МЕУ и ИАИЕУ в направление автентикация, оторизация на база данни от потребители и компютри включва управление на сигурността и правата в Windows Active Directory. Основни функционалности са свързани с автентикация, оторизация, прилагане и управление на политики на директорийни обекти включващи потребители, компютри и мейл услуга базирана на активна директория и др. Услугата се изразява в осигуряване на работоспособността, наблюдение, мониторинг и управление на информационно-комуникационната инфраструктура на МЕУ и ИАИЕУ с цел постигане на максимална ефективност, защита и информационна сигурност на МЕУ и ИАИЕУ. Услугата включва:

- Наблюдение в режим 24/7 на пощенската услуга и Активната директория;
- Предоставяне на препоръки за подобрения в пощенската услуга и Активната директория;
- Експертна помощ и реакция при инциденти свързани с пощенската услуга и Активната директория;

По-долу в настоящите технически параметри са описани детайлно всички дейности в обхвата на услугата и начина на предоставянето им.

Обхват и изисквания към изпълнението на услуга по управление и наблюдение на информационно-

***комуникационната инфраструктурата (ИКИ)* в направление автентикация, оторизация, организация на база данни от потребители и компютри**

При изпълнение на услугата, ВЪЗЛОЖИТЕЛЯТ и ИЗПЪЛНИТЕЛЯТ, определят отговорни лица/екипи (*Приложение 3 към услуга 2.3*). Услугата включва:

- регулярни дейности по управление и експлоатация на информационната и комуникационна инфраструктура (ИКИ) на МЕУ и ИАИЕУ, вкл. и 24/7 мониторинг на ИКИ.
- дейности и отговорности на екипите от ИЗПЪЛНИТЕЛЯ и ВЪЗЛОЖИТЕЛЯ при възникване на инциденти в ИКИ на МЕУ и ИАИЕУ.

При изпълнение на дейностите по управление и експлоатация на ИКИ следва да се осигури поддръжка, с която се гарантира безотказна работа на компонентите на изградената информационна и комуникационна инфраструктура на МЕУ и ИАИЕУ.

При управление и експлоатация на ИКИ на МЕУ и ИАИЕУ, вкл. и при възникване на инцидент в компонентите на изградената информационна и комуникационна инфраструктура, се спазва следното разпределение на отговорностите между екипите на МЕУ и ИАИЕУ и ИЗПЪЛНИТЕЛЯ за всички структури на МЕУ и ИАИЕУ (ЦУ, териториални структури, офиси, изнесени работни места) и цялата им инфраструктура:

✓ **Сървър за електронна поща**

(1) Регулярните дейности по поддръжка и прилагане на промени, архивиране на данни на мейл услугата, управление на конфигурационни промени са отговорност на екипа на ИО АД. Регулярните дейности за ежедневни прегледи, актуализации и поддръжка на пощенските кутии, прилагане на политики и права са отговорност на екипа на ИО АД. При подаване на заявка за промяна, същата е съпроводена с попълнена форма за съответната промяна (*Приложение 1 към услуга 2.3*).

(2) При възникване на инциденти разпределението на отговорностите между екипите е както следва:

- За екипа на ИАИЕУ – ежедневни задачи свързани с обслужване на крайни потребители (Level 1 Helpdesk) на МЕУ и ИАИЕУ.
- За екипа на ИО АД - нисък, среден и висок приоритет на инциденти

✓ **Активна директория, включително и сървърни операционни системи на МЕУ и ИАИЕУ, които не включват управление и менажиране на апликация/приложение.**

(1) Регулярните дейности по поддръжка и прилагане на промени, управление на конфигурационни промени са отговорност на екипа на ИО АД. Регулярните дейности за ежедневни прегледи, актуализации и прилагане на политики и права в активната директория са отговорност на екипа на ИО АД. При подаване на заявка за промяна, същата е съпроводена с попълнена форма за съответната промяна (*Приложение 1 към услуга 2.3*)

(2) При възникване на инциденти разпределението на отговорностите между екипите е както следва:

- За екипа на ИАИЕУ –ежедневни задачи, свързани с обслужване на крайни потребители (Level 1 Helpdesk) на МЕУ и ИАИЕУ
- За екипа на ИО АД – нисък, среден и висок приоритет на инциденти

При възникване на инцидент, се определя неговият приоритет, влияние и спешност от екипа на ВЪЗЛОЖИТЕЛЯ. В случай, че отговорният служител от ИО АД, който е поел решаването на инцидента, прецени, че приоритета е зададен погрешно или въздействието е погрешно преценено, служителят от ИО АД е в правото си да промени приоритета на инцидента. Приоритетът на всеки инцидент определя времето, за което той следва да бъде разрешен. Приоритетът се определя от влиянието на инцидента върху крайните потребители и спешността, с която следва да бъде разрешен.

Влияние на инцидент		
Стойност	**Влияние**	**Описание**
1	Ниско	При въздействие върху единични потребители.
2	Средно	При въздействие върху отдел или локация.
3	Високо	Услугата не е налична за всички потребители.

Спешност при инцидент		
Стойност	**Спешност**	**Описание**
1	Ниска	Инцидент, при който не е засегната функционалност на услугата.
2	Средна	Инцидент, при който не е засегната основна функционалност на услугата.
3	Висока	Инцидент, при който е засегната основна функционалност на услугата.

Приоритетът се изчислява по формулата: **Приоритет = Влияние * Спешност**, както е показано по-долу:

Влияние / Спешност	**Ниско (1)**	**Средно (2)**	**Високо (3)**
Ниска (1)	1	2	3
Средна (2)	2	4	6
Висока (3)	3	6	9

Приоритет на инцидент	**Стойност**
1-2	Нисък (1)
3-6	Среден (2)
9	Висок (3)

Време за реакция при инцидент и Време за разрешаване на инцидент:

Времето за реакция при инцидент обхваща периода от докладването на инцидента от ВЪЗЛОЖИТЕЛЯ до момента на неговото приемане от ИО АД. Докладването на инцидента може да става по следните канали:

- чрез регистрирането му в системата за управление на заявки на ИО АД;
- по електронна поща до координатора по договора от ИО АД или други оправомощени лица;
- по телефон – само при инциденти с критичен приоритет, като това не отменя регистрирането на инцидента в системата за управление на заявки на ИО АД;

Времето за разрешаване на инцидент обхваща периода от започната работа по инцидента от служител на ИО АД до момента на възстановяване нормалната работа на услугата. Времената са обвързани със стойността на параметъра **приоритет на инцидента**, както е показано по-долу:

Приоритет	**Време за реакция**	**Време за разрешаване**
Нисък (1)	До 4 часа	До 5 раб. дни
Среден (2)	До 2 часа	До 3 раб. дни
Висок (3)	До 45 минути	До 1 раб. ден

3. Параметри на услугата по управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ)

За осигуряване параметрите на услугата ИЗПЪЛНИТЕЛЯТ поддържа екипи от специалисти за обслужване на потребителите на услугата и наблюдение на услугата. Дейностите, свързани с инсталиране на новодоставен софтуер, хардуер и съпровождащите ги или нови лицензи са част от дейностите извършвани от ИО АД и не подлежат на допълнително заплащане в срока на договора. Дейностите, свързани с администриране и управление на информационните и комуникационните системи на МЕУ и ИАИЕУ се осъществяват отдалечено, чрез защитен криптиран канал – VPN.

При изпълнението на услугата като цяло ИО АД следва да осигури:

- Екипът на ИО АД информира незабавно екипа на ВЪЗЛОЖИТЕЛЯ за отпадане на някой от описаните елементи в ИКИ на МЕУ и ИАИЕУ с цел предприемане на последващи действия от ВЪЗЛОЖИТЕЛЯ.
- Оказване на съдействие и техническа помощ на ИТ екипа на ВЪЗЛОЖИТЕЛЯ при прилагане на политики по сигурност в комуникационната инфраструктура на МЕУ и ИАИЕУ.
- Оказване на техническа и системна помощ на ИТ екипа на ВЪЗЛОЖИТЕЛЯ при необходимост от изменения и/или изграждане на нови VPN връзки към други организации.
- Мониторинг и анализ на основните компоненти на изградената централизирана информационна и комуникационна инфраструктура на МЕУ и ИАИЕУ.

- Проверка за актуализации, както и инсталирани критични пачове след потвърждение от ВЪЗЛОЖИТЕЛЯ.
- Диагностика и препоръки за актуализация на основните компоненти на изградената информационна и комуникационна инфраструктура на Министерство на електронното управление и Изпълнителна агенция „Инфраструктура на електронното управление“.
- Техническа консултация по оптимизация и развитие на комуникационната инфраструктура.
- Актуализация на физическата и логическата информационна и комуникационна инфраструктура.
- Екипът на ВЪЗЛОЖИТЕЛЯ има достъп до всички нива на ИКИ, както и прилагането на промените и конфигурациите в цялата ИКИ се извършват съгласувано с екипа на ВЪЗЛОЖИТЕЛЯ и след тяхно потвърждаване.
- При необходимост екип от специалисти в офис, посочен от ВЪЗЛОЖИТЕЛЯ
- Професионалните компетенции на екипа включващи следната подготовка, курсове и сертификация в следните направления, като минимум:
    - 2xМрежови архитекти - CCIE Enterprise, CCNP Enterprise / 350-401 ENCOR
    - 2xMicrosoft експерти - MS-900/AZ-900
    - 1xThreat Intelligence експерт - SANS FOR 578
    - 1xAdvance Network Forensics експерт- SANS FOR 572
    - 1xReverse-Engineering Malware експерт – SANS FOR 610
    - 1xAdvanced Incident Response, Threat Hunting and Digital Forensics експерт - SANS FOR 508
    - 1xEnterprise-Class Incident Response & Threat Hunting експерт - SANS FOR 608
    - 1xCybersecurity Engineering: Advanced Threat Detection and Monitoring експерт - SANS SEC 511
    - 1xSecurity Leaderships for Managers SANS LDR 512
    - 2xSecurity Operation Analyst SC200
    - 1x PMP – Project Management Professional

1x PMI-ACP

При необходимост, ИЗПЪЛНИТЕЛЯТ ще осигури екип от системни администратори с отдалечено работно място, в офис на ВЪЗЛОЖИТЕЛЯ. В случай на инцидент със сигурността, изискващ посещение на място, мястото на изпълнение се посочва от ВЪЗЛОЖИТЕЛЯ.

Режим на услугите е периода, в който услугите се ползват и е налична поддръжка за тях. Всички критични услуги по трите дейности дефинирани от ВЪЗЛОЖИТЕЛЯ или идентифицирани като такива от ИО АД и детайлно описани по темплейта в *Приложение 4*, са в режим на поддръжка и наблюдение 24x7x365. За определяне на наличност на услугите, ИЗПЪЛНИТЕЛЯТ инсталира система за мониторинг на системите и услугите на ВЪЗЛОЖИТЕЛЯ. Наличността на услугите, описани в

обхват на дейността и отговорност на ИО АД, се определя на база отчетен период, като средната стойност е минимум 99.5% като се изключва времето за актуализации и планирани профилактики. Графикът на прекъсванията регламентира часовия интервал, в който услугата може да бъде планирано прекъсната за профилактика и/или актуализация. При установена необходимост за планирано прекъсване на услугата, ръководителят по договора от ИО АД или отговорник за изпълнение на промяната от екипа на ИО АД уведомява ВЪЗЛОЖИТЕЛЯ. Непланирани прекъсвания се класифицират като инцидент. Максималното време за прекъсване регламентира времето, за което услугата може да бъде прекъсната в регламентирания часови интервал, съгласно графика на прекъсванията. Уведомяването при прекъсване регламентира минималното време, преди което трябва да бъде информирано МЕУ и ИАЕУ (когато е приложимо) за предстоящото прекъсване на услугата. Времето се съгласува с ВЪЗЛОЖИТЕЛЯ и варира в зависимост от критичността на изпълнение на промяната.

№	Параметър	Стойност	Забележка
1.	График на прекъсване	22:00 - 06:00 в работни дни или 10:00 – 08:00 в почивни дни	При планирани прекъсвания. При извънредни и критични ситуации, с цел запазване на наличността на услугата, се допуска извършването на планирани дейности в друг времеви интервал, но след писмено съгласуване между ВЪЗЛОЖИТЕЛЯ и ИО АД.

3. Приемане на услугата по управление и наблюдение на киберсигурността на информационно-комуникационната инфраструктура на Министерство на електронното управление (МЕУ) и Изпълнителна агенция „Инфраструктура на електронното управление“ (ИА ИЕУ), оперативно управление, наблюдение, ескалация, оперативна координация и реакция при инциденти на административни органи в Република България, както и управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ) на МЕУ и ИАИЕУ в направление автентикация, оторизация, организация на база данни от потребители и компютри

Приемането на услугите по управление, наблюдение и киберсигурност на информационно-комуникационната инфраструктура на МЕУ и ИАИЕУ се извършва с подписване на приемо-предавателен протокол, към който се прилага:

- За услугата за мониторинг по сигурността, наблюдение, докладване на киберинциденти и реакция при инциденти в режим 24*7*365:

- Доклад за открити уязвимости във вътрешната мрежа за управление на МЕУ и ИАИЕУ за всеки месец;
- Доклад за открити уязвимости в публичните мрежи на МЕУ и ИАИЕУ, в който влизат публични услуги на МЕУ и ИАИЕУ за всеки месец;
- Детайли за всички генерирани аларми и предприети действия за всеки месец;
- Детайли за всички генерирани аларми и предприети действия за всеки месец за публичната администрация;
- Доклади от анализа на атаки или зловредни файлове и др.;
- Доклад за открити уязвимости в публичните мрежи на публичната администрация (Vulnerability and ASM Report);
- Доклад за извършени търсения на компрометирани системи и мрежи (Threat Hunting Report);
- Доклади за открити изтекли данни, компрометирани системи, анализи на хакерски групи, техники на атака (Threat Intelligence Report);
- Доклади за инциденти, тяхното смекчаване и реакция;
- Доклад от инструмент за оценка на състоянието на сигурността на средата на Active Directory . Доклада идентифицира неправилни конфигурации, уязвимости и рискове, които атакуващите биха могли да експлоатират.
- Доклади за мейл поток, активности по мейл, доклади и извадки от съществуващи системи за защита на поща.
- Услугата по управление и наблюдение на информационно-комуникационната инфраструктурата (ИКИ): доклад, който включва всички изпълнени дейности в тримесечния период.

ПРИЛОЖЕНИЕ 1

CHANGE CONTROL REQUEST FORM			
ДАТА:		**ЗАЯВИТЕЛ(И)**	

КЛИЕНТ		**ПРОЕКТ**			
ИНЦИДЕНТ #		**ИСКАНЕ ЗА ПРОМЯНА**		**ПРИОРИТЕТ**	
ТЕМА					
ЗАСЕГНАТИ СИСТЕМИ / ПРИЛОЖЕНИЯ					

ПРИЧИНА ЗА ЗАЯВКАТА

ПОЛЗИ ОТ ЗАЯВКАТА

ДЕТАЙЛНО ОПИСАНИЕ НА ПРОБЛЕМИТЕ И ПРИЧИНИТЕ ЗА ИСКАНИТЕ ПРОМЕНИ

ПРИЛОЖЕНИ ДОКУМЕНТИ		
No.	**ИМЕ**	**ОПИСАНИЕ**

ПРИЛОЖЕНИ ДОКУМЕНТИ		
No.	**ИМЕ**	**ОПИСАНИЕ**

ПЛАН ЗА ИЗВЪРШВАНЕ НА ПРОМЕНИ / ОТСТРАНЯВАНЕ НА ПРОБЛЕМИ					
No.	**ДЕЙСТВИЕ**	**РИСК / ВЛИЯНИЕ**	**ИЗПЪЛНИТЕЛ**	**ДАТА**	**НАЧ.ЧАС / КР.ЧАС**

КРИТЕРИИ ЗА УСПЕШНО ИЗВЪРШВАНЕ НА ПРОМЕНИ / ОТСТРАНЯВАНЕ НА ПРОБЛЕМИ					
No.	**КРИТЕРИЙ**	**УСЛОВИЕ ЗА ПРИЕМАНЕ**	**ПРОВЕРЯВАЩ**	**ДАТА**	**НАЧ.ЧАС / КР.ЧАС**

ПЛАН ЗА ВРЪЩАНЕ В ПЪРВОНАЧАЛНО СЪСТОЯНИЕ ПРИ НЕУСПЕШНО ИЗВЪРШВАНЕ НА ПРОМЯНА					
No.	**ДЕЙСТВИЕ**	**РИСК / ВЛИЯНИЕ**	**ИЗПЪЛНИТЕЛ**	**ДАТА**	**НАЧ.ЧАС / КР.ЧАС**

СПИСЪК ЗА СЪГЛАСУВАНЕ / ОДОБРЕНИЕ / ПРИЕМАНЕ						
No.	**ИМЕ**	**КОМПАНИЯ**	**E-mail**	**СЪГЛАСУ-ВАНЕ**	**ОДОБРЕНИЕ**	**ПРИЕМА-НЕ**

ПРИЛОЖЕНИЕ 2

	ДЕЙНОСТ	**ЕКИП ИО**	**ЕКИП МЕУ**
1	действа като звено за контакт по въпроси, свързани с мрежовата и информационната сигурност на национално ниво и по оперативни въпроси на международно ниво;		X
2	подпомага дейностите по създаването на секторните екипи за реагиране при инциденти с компютърната сигурност	X*	X
3	участва в изграждането и дейностите на Националната мрежа на екипите за реагиране при инциденти с компютърната сигурност	X*	X
4	обобщава и анализира предоставената информация от секторните екипи за реагиране при инциденти с компютърната сигурност и изготвя доклади в случай на необходимост	X*	X
5	предоставя съвети и препоръки на органите на държавната власт, органите на местното самоуправление и юридическите лица, създадени със специален закон, по важни въпроси, свързани с мрежовата и информационната сигурност;		X
6	оказва експертна подкрепа на административните органи и на други юридически лица при изграждане, внедряване и поддържане в актуално състояние на системи за управление на информационната сигурност съгласно националните и международните стандарти в тази област		X
7	участва в разработването и тестването на национални и по линия на Европейския съюз и НАТО стандартни оперативни процедури		X
8	при възникване на инциденти в мрежовата и информационната сигурност дава препоръчителни указания на административните органи, на националните компетентни органи и на секторните екипи за реагиране при инциденти с компютърната сигурност	X*	X
9	информира незабавно Националното единно звено за контакт за уведомленията за трансгранични инциденти със значително увреждащо въздействие и за трансгранични инциденти със съществено въздействие, подадени съгласно този закон, и в	X*	X

	случай на необходимост иска съдействие от Националното единно звено за контакт за тяхното разрешаване;		
10	участва в международни мрежи за сътрудничество	X*	X
11	Security Incident Management - Управление на инциденти, свързани със сигурността. Координацията и управление на настъпили инциденти е с обхват цялата публична администрация	X	X
12	Security Analysis - анализ на различни елементи и фази от кибератаки напр. (анализ на malware и др.).Извършване на последващ контрол, координирано с ЕЦК на МЕУ и/или ИА ИЕУ за отстранени инциденти при необходимост. Анализът е на база получен артефакт независимо от административната единица	X	
13	Security Audit - преглед на актуално състояние на киберсигурност и даване на препоръки в случай на новоизлезли уязвимости или координирани прегледи.	X	X
14	Vulnerability Management and Patch Management - Ежемесечна автоматизирана проверка за наличие на уязвимости в публично видимите услуги на публичната администрация, проактивно откриване на повърхности на атака и последващо изготвяне на план и препоръки за тяхното смекчаване.	X	
15	Threat Hunting – проактивно търсене на компрометирани системи и услуги с цел ранно откриване на инциденти в публичната администрация.	X	
16	Threat Intelligence – мониторинг на киберобстановката в Република България относно хакерски групи, изтекли данни и акаунти, нови техники и тактики на атака и изграждане на threat profile за различните сектори и национално ниво. Услугата обхваща всички административни единици и публичната администрация.	X	
17	Incident Response – откриване на кибератаки и възстановяване от инциденти за всички административни единици в публичната администрация. Съобщаване на установени инциденти до 1 работен ден с конкретни препоръки за отстраняването им. Установяване на	X	

	кореновата причина за наличието на инцидент, извършване на корелационен анализ и препоръки за отстраняване.		
	X* - Подпомагане на екипа на МЕУ при нужда с допълнителните задачи и експертна помощ		

ПРИЛОЖЕНИЕ 3

СПИСЪК НА ОТГОВОРНИТЕ ЛИЦА ПО ЗАЯВКА						
No.	**ИМЕ**	**КОМПАНИЯ**	**Е-МЕЙЛ**	**ТЕЛЕФОН**	**ОТДЕЛ**	**ОТГОВОРНОСТИ**

ПРИЛОЖЕНИЕ 4

СПИСЪК НА КРИТИЧНИТЕ АКТИВИ НА ВЪЗЛОЖИТЕЛЯ					
No.	**АКТИВ**	**СИСТЕМА**	**ПРИЛЕЖАЩИ КОМПОНЕНТ**	**IP АДРЕС**	**НАЛИЧНОСТ В %**

Приложение №2

към Договор № ……

(Образец)

Д Е К Л А Р А Ц И Я
ЗА ОПАЗВАНЕ НА ИНФОРМАЦИЯ

Долуподписаният/ та ……..,
ЕГН: .....,[10] в качеството ми на ……., декларирам, че ще пазя в тайна, станалата ми известна във връзка с изпълнението на Договор № ……/…..... г.[11] информация, съдържаща данни, представляващи данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация. За неизпълнение на тези задължения ми е известно, че нося предвидената в съответните нормативни актове отговорност.

Запознат/а съм с разпоредбата на чл. 270 от *Данъчно-осигурителния процесуален кодекс*, съгласно която, ако разглася, предоставя, публикувам, използвам или разпространя по друг начин факти и обстоятелства, представляващи данъчна и осигурителна информация, ако не подлежа на по-тежко наказание, ще бъда наказан/а с глоба от 1000 лв. до 5000 лв., а в особено тежки случаи - от 5000 лв. до 10 000 лв.

Декларирам, че ще пазя в тайна, станалата ми известна информация, относно съдържанието на документация, вътрешни правила, процедури, организация, структура, начин на функциониране, комуникации, мрежи и информационни системи на Министерство на електронното управление и Изпълнителна агенция „Инфраструктура на електронното управление“, изготвени в хода на изпълнението документи и/или всякакви други постигнати резултати от изпълнението, както и че няма да разгласявам, използвам или предоставям на трети лица разработена в полза на ВЪЗЛОЖИТЕЛЯ документация или програмен код в явен и изпълним вид във връзка с изпълнението на този договор, с изключение на случаите, когато съм задължен по закон за това.

---

[10] *В случай, че лицето е чужденец, се вписват съответните идентификационни данни.*

[11] *Вписва се референтен номер на Договора, в договорния регистър на ВЪЗЛОЖИТЕЛЯ.*

При обработването на данните се задължавам да спазвам разпоредбите на *Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО* и *Закона за защита на личните данни*.

Известна ми е отговорността по чл. 284 от *Наказателния кодекс*, а именно: налагане на наказание лишаване от свобода до две години или пробация, ако във вреда на държавата, на предприятие, организация или на частно лице съобщя другиму или обнародвам информация, която ми е поверена или достъпна по служба и за която зная, че представлява служебна тайна.

Ще спазвам изискванията на действащата нормативна уредба в областта на мрежовата и информационната сигурност.

Известна ми е отговорността по Глава 9а от Особената част на *Наказателния кодекс*, относно достъп до компютърни данни в компютърна система без разрешение, добавяне, промяна, изтриване или унищожаване на компютърна програма или компютърни данни, въвеждане на компютърен вирус в компютърните системи или мрежи на МЕУ и ИАИЕУ, разпространение на пароли или кодове за достъп до компютърна система или до компютърни данни и от това последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна.

Подпис:

(подписване с електронен подпис)