Договор
№16138

Днес, 05.12.2018 г. в „ТЕЦ Марица изток 2“ ЕАД, се сключи настоящият Договор за възлагане на обществена поръчка между:

„ТЕЦ Марица изток 2” ЕАД, със седалище и адрес на управление: област Стара Загора, община Раднево, с. Ковачево, п. код 6265, тел.: 042/662214, факс: 042/662000, Електронна поща: tec2@tpp2.com, Интернет страница: www.tpp2.com; регистрирано в търговския регистър при Агенцията по вписванията; ЕИК 123531939; Разплащателна сметка: IBAN: BG22TTBB94001526680953, BIC: TTBBBG22, „Сосиете Женерал Експресбанк“ АД, представлявано от инж. Живко Димитров Динчев – Изпълнителен директор, наричано за краткост Възложител

и

„Киберсек“ ДЗЗД, гр. София, със седалище и адрес на управление: област София – град, община „Столична“, гр. София, район „Студентски“, п. код 1700, ул. Проф. Саздо Иванов №6, ет.3; телефон: 02/9621371; факс: 029624715; Електронна поща: ppetrov@rct.bg, ЕИК: 177289344; IBAN: BG78UNCR70001523336912, BIC: BGUNCRSF, „УниКредит Булбанк“ АД, гр. София, представляван от Петър Цолов Петров - Представляващ, наричано за краткост Изпълнител

Съдружници в дружеството:

- „Рад група-комуникационни технологии“ ООД, гр. София, ЕИК 831508150 с дял 34.00%
- „Атлас ко“ ООД, гр. София, ЕИК 831820997 с дял 33.00 %
- „Екинокс Глобал Сълюшънс“ ЕООД, гр. София, ЕИК 204725699 с дял 33.00%

за следното:

Член 1. Предмет

1.1.Възложителят възлага, а Изпълнителят приема да осъществи **Изграждане на център за киберсигурност за нуждите на „ТЕЦ Марица изток 2“ ЕАД. Усъвършенстване на съществуващата система за личните данни и създаване на надеждна киберзащита за нея в изпълнение на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г.**

1.2.Предметът на договора включва изпълнението на следните дейности:

1.2.1.Преработване на съществуващите компютърни мрежи и изграждане на три нови компютърни мрежи: „Производствена”, „Административна” (съставена от две отделни части с различни функционални характеристики) и „Публична” компютърна мрежа, която включва:

1.2.1.1.Доставяне, монтаж и конфигуриране на мрежово оборудване за изграждане на:

а)опорна комуникационна мрежа за създаване на основен Data Center;

б)резервен Data Center;

в)комуникационна инфраструктура;

г)комуникационни възли;

1.2.1.2.Доставяне, монтаж и конфигуриране на мрежово оборудване за изграждане на три нови компютърни мрежи:

а)„Производствена”;

б)„Административна” (съставена от две отделни части с различни функционални характеристики)

в)„Публична”

1.2.1.3.Преобразуване на съществуващите персонални компютри във виртуални работни станции (терминали);

1.2.1.4.Закупуване на необходимите различни софтуерни продукти и лицензи.

1.2.2.Изграждане на клъстерна сървърна система, състояща се от 4 броя основни и 4 броя резервни виртуални сървъри. Апликации и архивиране на информацията в основния и резервния дейта център, които включват:

1.2.2.1.Доставяне, инсталиране и конфигуриране на клъстерна сървърна система (сървъри и софтуер);

1.2.2.2.Система за съхранение на информацията (Storage system);

1.2.2.3.Активно оборудване за изграждане на LAN / SAN сървърна мрежа (за основен и резервен Data Center);

1.2.2.4.Закупуване на необходимите различни софтуерни продукти и лицензи.

1.2.3.Изграждане на система за киберсигурност, което включва:

1.2.3.1.Доставяне, инсталиране и конфигуриране на:

а)външна защитна стена, предоставяща софтуер за защита от злонамерени файлове, достъп до злонамерени домейни и „С и С” трафик и защита на уязвими места;

б)вътрешна защитна стена;

в)хардуер и софтуер за съвременна защита на сървърите и работните станции;

г)приложение за уеб - сигурност;

д)професионално приложение за сигурност на електронната поща;

е)мрежови Phase 3 контрол на достъпа;

ж)система за защита от изтичане на данни;

з)система за мониторинг на системата за киберсигурност;

1.2.3.2. Усъвършенстване на система за защита на личните данни;

1.2.3.3.Закупуване на необходимите различни софтуерни продукти и лицензи.

1.3.Изпълнителят се задължава да изпълни дейностите по алинея 1.1 и алинея 1.2 в съответствие с изискванията на Приложение №1 – Технически изисквания и Приложение №2 - Схемата за класификация на етапите за сключване и изпълнение на договор, които са неразделна част от настоящия договор.

1.4.Настоящият договор е сключен в резултат на проведена процедура на договаряне с публикуване на обявление за поръчка за възлагане на обществена поръчка с рег.№ 18073.

Член 2. Цена

2.1.Общата стойност на договора е **7 596 320.00 лв.** /седем милиона петстотин деветдесет и шест хиляди триста и двадесет лева/, без ДДС и включва:

2.1.1. Цена за изпълнението на Първи етап – Проектиране (предпроектно проучване и изработване на работни проекти) - **759 632.00 лв.** /седемстотин петдесет и девет хиляди шестстотин тридесет и два лева /, без ДДС.

2.1.2. Цена за изпълнението на Втори етап – Преработване на съществуващите компютърни мрежи и изграждане на 3 нови компютърни мрежи: „Производствена“, „Административна“ (съставена от 2 отделни части) и „Публична“ компютърна мрежа. Изграждане на компютърна мрежа от виртуални работни станции - **1 519 264.00 лв.** /един милион петстотин и деветнадесет хиляди двеста шестдесет и четири лева/, без ДДС.

2.1.3. Цена за изпълнението на Трети етап – Изграждане на клъстерна сървърна система, която се състои от 4 броя основни и 4 броя резервни виртуални сървъри - **1 671 190.40 лв.** /един милион шестстотин седемдесет и една хиляди сто и деветдесет лева и четиридесет стотинки/, без ДДС.

2.1.4. Цена за изпълнението на Четвърти етап – Изграждане на апликации и сторидж система за съхраняване на информацията в основния и резервния дейта центрове - **1 215 411.20 лв.** /един милион двеста и петнадесет хиляди четиристотин и единадесет лева и двадесет стотинки/, без ДДС.

2.1.5. Цена за изпълнението на Пети етап – Изграждане на система за киберсигурност - **2 278 896.00 лв.** /два милиона двеста седемдесет и осим хиляди осемстотин деветдесет и шест лева/, без ДДС.

2.1.6. Цена за изпълнението на Шести етап – Усъвършенстване на система за защита на личните данни - **151 926.40 лв.** /сто петдесет и една хиляди деветстотин двадесет и шест лева и четиридесет стотинки/, без ДДС.

Член 3. Начин на плащане

3.2.Плащането се извършва по банков път до 60 (шестдесет) дни след представяне на приемателните документи за всеки етап и фаза; оригинална фактура, издадена съгласно разпоредбите на чл.113 от ЗДДС и документи по чл.66, ал.4-7 от ЗОП при сключени договори с подизпълнители, както следва:

3.2.1.Първи етап – Проектиране (предпроектно проучване и изработване на работни проекти) - 10 % от общата стойност на договора.

3.2.2.Втори етап – Преработване на съществуващите компютърни мрежи и изграждане на 3 нови компютърни мрежи: „Производствена“, „Административна“ (съставена от 2 отделни части) и „Публична“ компютърна мрежа. Изграждане на компютърна мрежа от виртуални работни станции – 20 % от общата стойност на договора:

3.2.2.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи - 80 % от общата стойност на етапа;

3.2.2.2.Втора фаза – Преработване на съществуващите и изграждане на 3 нови компютърни мрежи. Изграждане на компютърна мрежа от виртуални работни станции – 20 % от общата стойност на етапа.

3.2.3.Трети етап – Изграждане на клъстерна сървърна система, която се състои от 4 броя основни и 4 броя резервни виртуални сървъри - 22 % от общата стойност на договора:

3.2.3.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи - 80 % от общата стойност на етапа;

3.2.3.2.Втора фаза – Изграждане на клъстерна сървърна система, която се състои от 4 броя основни и 4 броя резервни виртуални сървъри – 20 % от общата стойност на етапа.

3.2.4.Четвърти етап – Изграждане на апликации и сторидж система за съхраняване на информацията в основния и резервния дейта центрове – 16 % от общата стойност на договора:

3.2.4.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи - 80 % от общата стойност на етапа;

3.2.4.2.Втора фаза – Изграждане на апликации и сторидж система за съхраняване на информацията в основния и резервния дейта центрове – 20 % от общата стойност на етапа.

3.2.5.Пети етап – Изграждане на система за киберсигурност – 30 % от общата стойност на договора:

3.2.5.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи - 80 % от общата стойност на етапа:

3.2.5.2.Втора фаза – Изграждане на система за киберсигурност – 20 % от общата стойност на етапа.

3.2.6.Шести етап – Усъвършенстване на система за защита на личните данни – 2 % от общата стойност на договора:

3.2.6.1.Първа фаза – Доставяне на необходимите софтуер и лицензи – 80 % (осемдесет на сто) от общата стойност на етапа;

3.2.6.2.Втора фаза - Усъвършенстване на система за защита на личните данни. Изработване на необходимата документация – 20 % от общата стойност на етапа.

Срокът за плащане започва да тече от датата на последно представения документ.

Член 4. Срокове и място на доставка

4.1.Срокът за изпълнение на договора е до 24 (двадесет и четири) месеца от датата на подписване на договора и е разделен на етапи, както следва:

4.1.1.Първи етап – Проектиране (предпроектно проучване и изработване на работни проекти).

Срок – до 4-ия месец след подписване на договора.

4.1.2.Втори етап – Преработване на съществуващите компютърни мрежи и изграждане на 3 нови компютърни мрежи: „Производствена“, „Административна“ (съставена от 2 отделни части) и „Публична“ компютърна мрежа. Изграждане на компютърна мрежа от виртуални работни станции:

4.1.2.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи.

Срок – до 8-мия месец след подписване на договора.

4.2.2.Втора фаза – Преработване на съществуващите и изграждане на 3 нови компютърни мрежи. Изграждане на компютърна мрежа от виртуални работни станции.

Срок – до 12-тия месец след подписване на договора.

4.1.3.Трети етап – Изграждане на клъстерна сървърна система, която се състои от 4 броя основни и 4 броя резервни виртуални сървъри:

4.1.3.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи.

Срок – до 12-тия месец след подписване на договора.

4.1.3.2.Втора фаза – Изграждане на клъстерна сървърна система, която се състои от 4 броя основни и 4 броя резервни виртуални сървъри.

Срок - до 14-тия месец след подписване на договора.

4.1.4.Четвърти етап – Изграждане на апликации и сторидж система за съхраняване на информацията в основния и резервния дейта центрове:

4.1.4.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи.

Срок – до 14-тия месец след подписване на договора.

4.1.4.2.Втора фаза – Изграждане на апликации и сторидж система за съхраняване на информацията в основния и резервния дейта центрове.

Срок – до 16-тия месец след подписване на договора.

4.1.5.Пети етап – Изграждане на система за киберсигурност:

4.1.5.1.Първа фаза – Доставяне на необходимите хардуер, софтуер и лицензи.

Срок – до 16-тия месец след подписване на договора.

4.1.5.2.Втора фаза - Изграждане на система за киберсигурност.

Срок – до 24-тия месец след подписване на договора.

4.1.6.Шести етап – Усъвършенстване на система за защита на личните данни. Документация, софтуер и лицензи:

4.1.6.1.Първа фаза – Доставяне на необходимите софтуер и лицензи.

Срок – до 16-тия месец след подписване на договора.

4.1.6.2.Втора фаза – Усъвършенстване на система за защита на личните данни. Изработване на необходимата документация.

Срок – до 24-тия месец след подписване на договора.

4.2.Мястото за доставяне на стоката и изпълнението на услугата е „ТЕЦ Марица изток 2“ ЕАД

Член 5.Приемане на изпълнението

5.1.Работният проект трябва да бъде предаден за одобрение на Възложителя в 3 (три) екземпляра на хартиен и 1 (един) екземпляр на магнитен носител на български език. При наличие на класифицирана информация в работния проект да се спазват изискванията на ЗЗКИ, като класифицираната част се обособи в отделно приложение към работния проект.

5.2.Приемането на работния проект се извършва на Технически съвет на Възложителя.

5.3.Доставката на необходимите хардуер, софтуер и лицензи се приема с примо-предавателен протокол.

5.4.Въвеждане в експлоатация:

5.4.1.След завършване на монтажните и инсталационните работи, компютърните мрежи, клъстерната сървърна система, системата за съхранение на информацията и системата за киберсигурност трябва да бъдат настроени и тествани.

5.4.2.След завършване на монтажните работи, настройките и тестването на компютърните мрежи, клъстерната сървърна система, системата за съхранение

на информацията и системата за киберсигурност, Изпълнителят трябва да проведе курс за обучение за работа с техническите средства и софтуера, с оторизирани представители, определени от Възложителя.

5.4.3.Изпълнителят предоставя на Възложителя Инструкция за експлоатация и Ръководство за работа с компютърните мрежи, клъстерната сървърна система, системата за съхранение на информацията и системата за киберсигурност на български език.

5.4.4.Изпълнителят осигурява и организира провеждането на изпитания на компютърните мрежи, клъстерната сървърна система, системата за съхранение на информацията и системата за киберсигурност с участието на технически експерт/и от страна на Възложителя.

5.4.5.Преди да бъдат въведени в експлоатация, **компютърните мрежи, клъстерната сървърна система, системата за съхраняване на информацията и системата за киберсигурност**, трябва да бъдат проведени 72 (седемдесет и две) - часови изпитания

5.4.6.За проведените изпитания и тестове на компютърните мрежи, клъстерната сървърна система, системата за съхранение на информацията и системата за киберсигурност трябва да се попълнят и подпишат всички необходими протоколи по установения ред.

5.5.Успешно преминалите обучението участници трябва да получат документ, удостоверяващ този факт.

Член 6. Права и задължения на Възложителя:

6.1. Възложителят има право:

6.1.1. във всеки момент от изпълнението на договора, да извършва проверка относно качеството, стадия на изпълнение, техническите спецификации и др.

6.1.2. във всеки момент от изпълнението на договора да дава предложения за допълнения и изменения с цел оптимизация, без да изменя предмета на договора.

6.1.3. да прави предложения във връзка с организацията на работния график, в случаите, в които за извършването на работата по настоящия договор е необходимо участието на Възложителя или на негови служители.

6.1.4. да изисква от Изпълнителя да сключи и да му представи договори за подизпълнение с посочените в офертата му подизпълнители.

6.2. Възложителят се задължава:

6.2.1. да плати на Изпълнителя уговорената цена в сроковете и при условията на настоящия Договор;

6.2.2. да окаже необходимото съдействие на Изпълнителя за изпълнение на възложената му работа, включително като предостави информация и достъп до данните, които Изпълнителят е изискал във връзка с изпълнение на задълженията си по настоящия Договор

6.2.3. да осигурява необходимия достъп и условия на работа при посещение на Изпълнителя или негови служители в офисите на Възложителя

6.2.4. да определи служител по сигурността на информацията на „ТЕЦ Марица изток 2“ ЕАД като лице по чл.105 от ЗЗКИ, което осъществява и контрол

по прилагането на специфичните изисквания по чл.10 от „НАРЕДБА за общите изисквания за гарантиране на индустриалната сигурност.“

Член 7. Права и задължения на Изпълнителя:

7.1.Изпълнителят има право:

7.1.1. при своевременно и точно изпълнение на задълженията си по настоящия договор да получи уговорената цена, в сроковете и при условията на този договор;

7.1.2. да изисква разяснения и информация от Възложителя във връзка с изпълнението на поетите задължения по настоящия договор;

7.1.3. да получава необходимото съдействие от Възложителя при изпълнение на задълженията си по този договор.

7.2.Изпълнителят се задължава:

7.2.1. да изпълни предмета на договора, посочен в член 1, съгласно Технически изисквания на Възложителя в сроковете и при останалите условия на този договор.

7.2.2. да изпълни възложената му работа така, че тя да бъде напълно годна и функционална за предвиденото в този договор предназначение.

7.2.3. да спазва указанията на Възложителя относно извършената работа

7.2.4. да се запознае с **Указания за реда и последователността при подготовка на документи за допускане до работа на външни изпълнители на територията на „ТЕЦ Марица изток 2” ЕАД,** публикувани на интернет страницата на дружеството (www.tpp2.com, Профил на купувача) и да изпълни изискванията им.

7.2.5. в еднодневен срок от подписване на договора да осъществи контакт с отговорника по договора и с негово съдействие да съгласува с компетентните лица на Възложителя от отдели „Сигурност и управление при кризи”, „Безопасност и здраве при работа”, „Технически контрол и качество” и „Екология”, както и РСПБЗН, необходимостта от представяне на документи за допускане до работа на територията на дружеството. Компетентните лица съгласуват подготвените от Изпълнителя документи и при липса на забележки подписват **Протокол за проверка на документи за допускане до работа.**

7.2.6. в случай че Териториална дирекция “Национална сигурност”, гр. Стара Загора не издаде разрешение за работа или извършване на конкретно възложена задача на лице – работник или служител на Изпълнителя, Изпълнителят се задължава да го замени, като предложи на Възложителя друго лице, притежаващо равностойна квалификация и опит, което също подлежи на проучване по горния ред.

7.2.7. да определи свои представител по чл.12, ал.1 от Наредбата за общите изисквания за гарантиране на индустриалната сигурност, което отговаря за прилагането на мерките за защита на класифицираната информация при изпълнението на Договора и оказва съдействие на лицето по чл.105 от ЗЗКИ.

7.2.8. да осъществи взаимодействие с компетентната служба за сигурност по чл.11, ал.2 и 3 от ЗЗКИ.

7.2.9. да забрани размножаване на класифицирана информация, освен при изрично съгласие на ВЪЗЛОЖИТЕЛЯ и в съответствие с изискванията на ЗЗКИ.

7.2.10. да предостави на съответната компетентна служба за сигурност по чл.11, ал.2 и 3 от ЗЗКИ, информация за лицата, чиято дейност изисква достъп до класифицирана информация.

7.2.11. да ограничи разпространяването на класифицирана информация до минимален брой лица в съответствие с принципа „необходимост да се знае.“

7.2.12. да поддържа актуален списък на лицата, получили разрешение за достъп до класифицирана информация във връзка с договора, съдържащ данни за датата на издаване на разрешението за достъп и срока на неговата валидност, нивото на класификация и обема на информацията, до която лицата имат достъп във връзка с изпълнението на договора и задачата, която изпълняват.

7.2.13. да отказва достъп до класифицирана информация на всяко лице, което не отговаря на изискванията на чл.3 от ЗЗКИ.

7.2.14. да задължи лицата, получили разрешение за достъп до класифицирана информация по договора, да подпишат декларации, с които се задължават да защитават информацията, станала им известна във връзка с изпълнението по договора и да носят отговорност при нерегламентиран достъп.

7.2.15. да уведоми незабавно съответната компетентна служба по чл.11, ал.2 и 3 от ЗЗКИ за всеки опит, осъществяване или съмнение за извършване на нерегламентиран достъп до класифицирана информация по договора, съмнение за извършено престъпление, свързано с нерегламентирания достъп до класифицирана информация по договора, както и за промени в обстоятелствата, послужили за издаване на удостоверението по чл.100 от ЗЗКИ.

7.2.16. да предоставя друга информация при поискване от съответната компетентна служба по чл.11, ал.2 и 3 от ЗЗКИ.

7.2.17. да ползва предоставената класифицирана информация само за цели, свързани с предмета на договора.

7.2.18. след приключване (прекратяване) на договора Изпълнителят е длъжен да върне цялата документация или материали, съдържащи класифицирана информация, получени от възложителя или създадени в хода на преговорите, сключването или изпълнението на договора при условията на чл.10, ал.2, т.13 от „НАРЕДБА за общите изисквания за гарантиране на индустриалната сигурност.“

7.2.19. Да спазва стриктно установените процедури при унищожаване на материали – носители на класифицирана информация.

7.2.20. Да предоставя класифицираната информация по договора на трета страна, само с изричното съгласие на източника на информация и при спазване изискванията на чл. 3 от ЗЗКИ.

7.2.21.да не разгласява информация за Възложителя, станала му известна при или по повод изпълнение на възложената му с този договор работа.

7.2.22. при изпълнение на възложената му с този договор работа, да не нарушава авторските и другите сродни права на трети лица и да спазва всички разпоредби на действащото българско законодателство във връзка със защита на правата на интелектуална собственост на трети лица. Изпълнителят гарантира, че софтуерните продукти, така както са доставени не накърняват никакви права на интелектуална собственост, притежавани от трети лица. Изпълнителят гарантира, че притежава всички необходими права на интелектуална собственост или за своя

сметка ще осигури законосъобразно придобиване на всички права и други съгласия, необходими му за изпълнение на предмета на договора

7.2.23. да предостави на Възложителя пълна документация на български език на електронен и/или хартиен носител;

7.2.24. да осигури гаранционна поддръжка при условията на този договор;

7.2.25. Изпълнителят е длъжен да уведоми възложителя за всякакви промени в предоставената информация в хода на изпълнението на поръчката.

7.2.26. Изпълнителят и подизпълнителя/и при изпълнението на договорите за обществени поръчки са длъжни да спазват всички приложими правила и изисквания, свързани с опазване на околната среда, социалното и трудовото право, приложими колективни споразумения и/или разпоредби на международното екологично, социално и трудово право съгласно приложение № 10 от ЗОП.

7.2.27. Изпълнителят се задължава да представи в срок от 10 дни, считано от датата на подписване на договора, договор за подизпълнение с подизпълнител/ите, посочени в офертата.

Член 8.Гаранционен срок и рекламации

8.1.Гаранционният срок е 12 месеца от датата на въвеждане в експлоатация на предмета на договора, удостоверено с подписване на протокол за 72 (седемдесет и две) - часови проби.

8.2.Изпълнителят гарантира, че доставеното от него оборудване отговаря на изискванията на Приложение №1 – Технически изисквания.

8.3.Възложителят има право на рекламации относно качеството на изделията по време на гаранционния срок, както всички разходи, свързани с отстраняване на дефекти са за сметка на Изпълнителя.

8.4.При поява на дефекти по време на гаранционния срок, се назначава двустранна комисия, която изготвя констативен протокол и се произнася за причините, породили дефектите и виновността за нанесените щети. Ако в тридневен срок от датата на уведомяване, Изпълнителят не изпрати свой представител за участие в комисията, Възложителят сам съставя протокола и той е задължителен за страните. При поправка на изделието гаранционният срок не тече за времето на отстраняване на дефекта. При замяна на некачественото изделие с ново гаранционният срок на доставеното изделие започва да тече от датата на доставката му.

8.5.Разходите за замяна или ремонт, за всички компоненти на Системата, както и всички други разходи за изпълнение на гаранционните задължения на място, включително за труд и транспорт, са за сметка на изпълнителя, ако се дължат на фабрични дефекти, на изпълнението на инсталационни и конфигурационни дейности и не са предизвикани от неправилна експлоатация.

8.6.Изпълнителят трябва да предостави софтуерните лицензи с включена поддръжка за 36 месеца.

8.7.Техническа поддръжка трябва да бъде достъпна по телефона, чрез електронна поща и/или уеб интерфейс 24 х 7.

8.8.Поддръжката трябва да включва софтуерни актуализации и надстройки, корекции на грешки, и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение.

8.9.Времето за отстраняване на възникнали проблеми и/или подмяна на неработещи модули е не повече от 48 часа.

8.10.Ако повреда на хардуера не може да бъде отстранена на място, ремонтът се извършва в оторизиран от производителя сервиз.

8.11.Ако повредата не може да бъде отстранена в рамките на не повече от 48 часа, Изпълнителят следва да предостави на Възложителя за времето на отстраняване на повредата, оборотно оборудване от същия функционален тип.

8.12.При невъзможност за отстраняване на повредата, отказалият хардуерен компонент трябва да се замени.

8.13.Компонентите на решението трябва да бъдат доставени от Изпълнителя.

8.14.След внедряване на продукта, Изпълнителят се задължава да осигури допълнително съдействие за срок от 3 месеца за фино донастройване на функционалните параметрите на Системата и допълване на оперативни сценарии за работа (use cases).

Член 9.Гаранция за изпълнение

9.1.Гаранция за изпълнение на договора - в размер на **379 816.00 лв**. /триста седемдесет и девет хиляди осемстотин и шестнадесет лева/. Представя се преди подписването на договора и се освобождава до 30 дни след изтичане на 12 месеца от гаранционния срок и отправено писмено искане от страна на Изпълнителя до Възложителя. Тази гаранция се връща на Изпълнителя при добросъвестно изпълнение и липса на претенции от страна на Възложителя.

9.2.Ако гаранцията е парична сума, се внася по сметката на Възложителя, а именно: IBAN BG22 TTBB 9400 1526 6809 53, BIC: TTBBBG22, "Сосиете Женерал Експресбанк" АД, клон Раднево.

9.3.Ако гаранцията е банкова, се представя по посочения в документацията образец и е със срок на валидност 37 месеца от датата на сключване на договора

9.4.Ако гаранцията е застраховка, се представя оригинална полица със срок на валидност 37 месеца от датата на сключване на договора

Член 10.Санкции и неустойки

10.1.Възложителят дължи на Изпълнителя неустойка в размер на законната лихва за забава, върху неиздължената сума на ден при забава на плащания по договора, но не повече от 5 % от стойността на забавената сума. Максималният размер на дължимите от Възложителя на това основание неустойки за забава се ограничава до 5 % от стойността на договора.

10.2.При забава изпълнителят дължи неустойка в размер на законната лихва за забава върху стойността на забавеното изпълнение, но не повече от 5% от стойността на договора.

10.3.При неточно изпълнение изпълнителят дължи неустойка в размер на 1% от стойността на договора за всеки установен случай на неточно изпълнение.

10.4.При пълно неизпълнение на задълженията си по договора Изпълнителят дължи неустойка в размер на 20% от стойността на договора.

10.5.При пълно неизпълнение или неточно изпълнение, Възложителят има право да изтегли гаранцията за изпълнение по чл.9 от настоящия договор.

10.6.Плащането на неустойки не лишава изправната страна по договора от правото и да търси обезщетения за претърпени вреди и пропуснати ползи над размера на неустойката.

10.7.Ако Възложителят прецени, че срока за изпълнение на договора не може да бъде спазен по причини, които се дължат изцяло или частично на негови действия или бездействия не налага предвидените в договора санкции и неустойки за определен от него период.

10.8.Изпълнителят се съгласява да удовлетвори претенциите на Възложителя за плащане на неустойки, настъпили в резултата на негово неизпълнение произтичащо от настоящият договор. Възложителят се задължава при възникване на претенция да уведоми писмено Изпълнителя. Уведомлението трябва да бъде мотивирано по основание и размер.

10.9.В случаите на алинея 10.8, Възложителят извършва прихващане между двете насрещни вземания, които се погасяват до размера на по-малкото, като клаузата произвежда правно действие при условие, че между страните съществуват насрещни, еднородни, заместими и изискуеми вземания.

Член 11.Форсмажор

11.1.Страните се освобождават от отговорност за частично или пълно неизпълнения на техните договорни задължения в случай, че невъзможността за изпълнение е следствие на събитие извън техния контрол, или в случай, че тези обстоятелства са упражнили непосредствено влияние върху изпълнението на този договор. В случай на възникване на такива форсмажорни обстоятелства съответните срокове се удължават с времето на действие на тези обстоятелства.

11.2.Всяка една от страните е длъжна да уведоми съответно другата страна за настъпването и прекратяването на форсмажорното събитие в 7 дневен срок от възникването и края на събитието, независимо от характера на събитието. Уведомяването трябва да е потвърдено от Българската търговско-промишлена палата. В случая намира приложение чл.306 от ТЗ.

Член 12.Разрешаване на спорове

12.1.Всички спорове породени от този Договор или отнасящи се до него, включително споровете, породени или отнасящи се до неговото тълкуване, недействителност, изпълнение или прекратяване, както и споровете за попълване празноти в Договора или приспособяването му към нововъзникнали обстоятелства, ако не могат да бъдат решени между страните се решават от компетентния съд.

Член 13.Прекратяване на договора

13.1.При наличие на "форсмажор", или друго събитие, двете страни могат да се споразумеят за прекратяване на договора.

13.2.Възложителят може да прекрати договора с едностранно 7-дневно писмено предизвестие, както и в следните случаи:

- На основание чл.118, ал.1, т.1 от ЗОП;

•При неизпълнение на задължението на Изпълнителя да представи в срок от 10 дни считано от датата на подписване на договора, договор за подизпълнение с подизпълнител/ите, посочени в офертата.

13.3.Когато Изпълнителят не изпълни някое свое задължение, поради причина за която отговаря, Възложителя може да прекрати Договора с петдневно писмено предизвестие. Неустойките по чл.10 остават дължими.

13.4.Възложителят има право да прекрати договора без предизвестие на основание чл.73, т.1 от ППЗОП.

ЧЛЕН 14. Защита на лични данни

14.1.Възложителят обработва лични данни за целите на сключване на настоящия договор от лицата, представляващи Изпълнителя съгласно чл.40 от ППЗОП. Данните се обработват на законово основание съгласно чл.112 във връзка с чл.67, ал.6 и чл.58 от ЗОП

14.2.Възложителят обработва лични данни за целите на изпълнение на настоящия договор за физическите лица, изпълняващи предмета на договора на територията на „ТЕЦ Марица изток 2“ ЕАД. Данните се обработват на законово основание съгласно ЗДАНС и ППЗДАНС и при спазване Указания за реда и последователността при подготовка на документи за допускане до работа на външни изпълнители на територията на „ТЕЦ Марица изток 2” ЕАД.

14.3.Възложителят по всяко време обработва личните данни по професионален начин, в съответствие с приложимото право и настоящия Договор, като прилага необходимите умения, грижа, старание и подходящо ниво на техническите и организационните стандарти за сигурност на данните.

14.4.Всяко разкриване или предаване на лични данни от някоя от страните по договора на трета страна е допустимо единствено, ако е необходимо за целите на сключване и изпълнение на настоящия договор, като трябва да е в съответствие с приложимото законодателство, по-специално член 25 и 26 на ОРЗД.

14.5.Когато това се изисква съгласно приложимото законодателство, всяка от страните информира засегнатите субекти на данните относно споделянето на лични данни съгласно настоящия договор. Получателят на данни незабавно уведомява разкриващата данни страна относно всякакви искания, възражения или всякакви други запитвания от субектите на данните по силата на приложимите закони относно обработването на лични данни, които могат да породят правно задължение или отговорност, или да засегнат по друг начин законните интереси на разкриващата данните страна.

14.6.Страните своевременно се уведомят и информират взаимно в случай на нарушаване на сигурността на лични данни или при искания на субекти на данни, надзорни органи или други трети страни, при условие, че събитието се отнася до обработването на лични данни и може да породи правно задължение или отговорност или да засегне по друг начин законните интереси на другата страна.

Член 15.Общи условия

15.1.Договорът влиза в сила от датата на неговото сключване.

15.2.Този договор се изготви и подписа в два еднообразни екземпляра, по един за всяка страна, при спазване на общите изисквания на Търговския закон, Закона за задълженията и договорите и Закона за обществените поръчки.

15.3.По всички въпроси, възникнали при изпълнението на настоящият договор, Изпълнителят се обръща към отговорника на договора, указан по-долу.

Възложител
Изп. директор: .....п.....
инж. Ж. Динчев

Изпълнител
Представляващ: .....п.....
П. Петров

Приложение 1

ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

за „Изграждане на център за киберсигурност за нуждите на „ТЕЦ Марица изток 2” ЕАД. Усъвършенстване на съществуващата система за личните данни и създаване на надеждна киберзащита за нея в изпълнение на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 година.”

Съдържание

Техническите изисквания са разработени в съответствие с приетите в „ТЕЦ Марица изток 2” ЕАД класифицирани документи до ниво „поверително”:

Дългосрочна ПРОГРАМА за осигуряване на киберзащитата и

Краткосрочен ПЛАН за осигуряване на киберзащитата.

I. Общи сведения и обхват

1. Общи сведения

Масовото използване на новите информационни технологии освен предимства, създава и условия за по-големи заплахи и уязвимост, които се

използват от различни лица (хакери), организирани престъпни групи, терористични структури и отделни държави.

Кибератаките и кибервойните не са насочени само към военни компютърни мрежи, информационни системи и средства, те засягат действието и на други държавни и частни структури с критично значение за нормалното функциониране на икономиката и обществото.

„ТЕЦ Марица изток 2" ЕАД е ключово звено в енергийната система на Република България, със съществен принос за нейния цялостен капацитет. Съгласно Решение № 755 от 21.09.2004 г. и Постановление № 181 на МС от 20.07.2009 г. и постановление № 3 от 10.01.2013 г., „ТЕЦ Марица изток 2" ЕАД е определен като стратегически обект от национално значение предвид решаващата му роля за стабилността на енергийната система.

В съответствие с Националната стратегия за киберсигурност „Киберустойчива България 2020" и в изпълнение на утвърдената Стратегия за управление на сигурността в „ТЕЦ Марица изток 2" ЕАД, както и на различни вътрешни нормативни документи, правилници, инструкции и заповеди на Ръководството на централата, в експлоатираните компютърни мрежи са включени конкретни хардуерни устройства и софтуерни модули за противодействие на различни кибератаки.

Въпреки предприетите действия, използваните от топлоелектрическата централа компютърни мрежи (информационни системи) не са защитени достатъчно надеждно.

Осигуряването на надеждна киберзащита на компютърните мрежи (информационните системи) в „ТЕЦ Марица изток 2" ЕАД ще гарантира изпълнението и на изискванията на приетия Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 година за защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания.

2.Обхват

2.1.Предпроектно проучване.

2.2.Проектиране.

2.3.Доставяне на технически средства и софтуер.

2.4.Монтиране, инсталиране и тестване.

2.5.Въвеждане в експлоатация.

2.6.Обучение на специалистите за работа със системите.

2.7.Изработване на съпровождаща документация.

2.8.Гаранционно поддържане.

II. Съществуващо положение:

В „ТЕЦ Марица изток 2" ЕАД има изградени и пуснати в експлоатация 3 (три) компютърни мрежи. Те са проектирани и изграждани (разширявани,

допълвани, обновявани) през различни периоди, но основно след 2000 година, като във всяка мрежа има включени конкретни хардуерни устройства и софтуерни модули за противодействие на различни кибератаки, но въпреки това използваните от топлоелектрическата централа компютърни мрежи (информационни системи) не са защитени надеждно.

Към месец декември 2017 година съществуващите компютърни мрежи включват:

- ✓ 15 броя различни видове и модели сървъри, произведени от DELL и HP;
- ✓ 400 броя различни видове и модели персонални компютри (произведени от различни фирми);
- ✓ 54 броя различни видове и модели комуникатори, произведени от Cisco, Dell, Classic Automation (Hirschmann);
- ✓ около 25 [km] оптически кабел.

Използваните базови програмни продукти са:

- ✓ UNIX;
- ✓ QNX;
- ✓ Windows Server NT;
- ✓ Windows Server 2003;
- ✓ Windows Server 2008;
- ✓ Windows 2000;
- ✓ Windows NT;
- ✓ Windows XP Pro;
- ✓ Windows 7 Pro;
- ✓ Windows 10 Pro.

Използваните приложни програмни продукти са:

- ✓ Система за мониторинг на производствения процес;
- ✓ Система за мониторинг на пожарната безопасност - WinGuard;
- ✓ Система за контрол на достъпа;
- ✓ Система за нормативни документи - „Апис”;
- ✓ Счетоводна система - „Ажур”;
- ✓ Система за контрол на работното време - Собствена разработка;
- ✓ Система за труд и работна заплата - Собствена разработка;
- ✓ Складова система - Собствена разработка;
- ✓ Деловодна система - Собствена разработка.

Инсталираните персонални компютри имат различни свободни портове за връзка с други електронни устройства.

Наличието на толкова различни технически средства и програмни продукти в използваните компютърни мрежи е предпоставка за възникване на нови уязвимости в компютърните мрежи.

III. Цел

За изпълнение изискванията и разпоредбите на:

Доклад „Анализ на риска с цел установяване на заплаха или вреда в резултат на нерегламентиран достъп, терористична дейност или саботаж, както и влиянието и последиците при тяхното проявление. Подобряване на системата

организационни, физически и технически мерки за физическа и информационна защита на „ТЕЦ Марица изток 2” ЕАД, като стратегически обект от значение за националната сигурност” от 2012 година;

Регламента (ЕС) 2016 / 679 на Европейския парламент и на Съвета от 27.04.2016 година;

Националната стратегия за киберсигурност „Киберустойчива България 2020” (приета от Министерски съвет на Република България на 13.07.2016 година);

Писмо на Държавната агенция „Национална сигурност” с регистрационен № RB202002-001-04 / И-З-1085 от 24.07.2017 година;

Доклад от охранителното обследване УРИ: 327р - 6991 от 25.07.2017 година на Държавната агенция „Национална сигурност”;

„Стратегия за управление на сигурността на „ТЕЦ Марица изток 2” ЕАД” (Протокол № 39 от 15.08.2017 година);

Писмо на Държавната агенция „Национална сигурност” с регистрационен № И-1724 от 20.09.2017 година;

„Политика за управление на сигурността на Български енергиен холдинг” (писмо с регистрационен № 01-0652 от 28.09.2017 година);

Протокол от 07.12.2017 година Технически съвет за приемане на Обща концепция за киберсигурност на „ТЕЦ Марица изток 2“ ЕАД;

Писмо на Държавната агенция „Национална сигурност” с регистрационен № И-224 от 25.01.2018 година;

е необходимо да се проектират и изградят надеждни и ефективни три нови компютърни мрежи: „Производствена”, „Административна” (съставена от две отделни части с различни функционални характеристики) и „Публична” компютърна мрежа, клъстерна сървърна система, система за съхранение на информацията, система за защита на личните данни и система за киберсигурност.

На основата на най-добрите световни практики за сигурност в киберпространството и с продуктите на световно утвърдени производители на хардуер и софтуер да се гарантира бъдещата киберсигурност на „ТЕЦ Марица изток 2“ ЕАД.

IV. Технически изисквания и параметри:

1. Изисквания, свързани с планирането на проекта

1.1. Изпълнителят трябва да изготви и да поддържа актуален План за управление на проекта (ПУП) и свързаните с него планове (като приложения към него или като отделни документи), а именно План за управление на качеството, План за управление на риска и План за управление на конфигурациите и промените. Плановете следва да описват дейностите по управление на проекта, които изпълнителят възнамерява да извършва при изпълнението му.

1.2. Конфигурацията на хардуера и софтуера при тестване и при приемане на системите трябва да бъде документирана.

1.3. Изпълнителят трябва да предостави примерно първоначално описание на системата, както и подробно описание на начина, по който възнамерява да я внедри в инфраструктурата на „ТЕЦ Марица изток 2“ ЕАД.

1.4. Финализирана и детайлна версия на системата трябва да бъде предоставена преди започване на дейностите по инсталиране и конфигуриране на компонентите на Системата, след като Изпълнителят се е запознал в детайли с инфраструктурата на „ТЕЦ Марица изток 2“ ЕАД.

1.5. Изпълнителят трябва да предостави т. нар. пътни карти (road maps) за бъдещото разширяване на системата за киберсигурност, системата за информационна сигурност и системата за защита на лични данни на „ТЕЦ Марица изток 2” ЕАД, като всяка пътна карта включва препоръки относно внедряването на допълнителни компоненти, процедури и услуги, които разширяват възможностите за разпознаване, разследване и отговор на кибер-инциденти (като оценка на уязвимостите (vulnerabilities assessment), разследване на кибер престъпления (forensic investigation)).

1.6. Изпълнителят трябва да подпомогне „ТЕЦ Марица изток 2“ ЕАД при изготвяне на оценката на промяната и съответното документиране на промяната, в следствие на инсталиране и конфигуриране на софтуера и хардуера, преди започването на инсталирането и конфигурирането на устройствата (хардуер, софтуер).

1.7. Изпълнителят трябва да предостави План за инсталиране и конфигуриране на устройствата (хардуер, софтуер) преди започване на дейностите по инсталиране и конфигуриране.

1.8. Изпълнителят трябва да инсталира и конфигурира всички компоненти (софтуер, хардуер) на съответната Система.

1.9. Изпълнителят трябва да изготви първоначалния План за работа с всяка Система, описващ начина на работа и координиране на целия набор от инструменти с цел консистентно предоставяне на услугите на Центъра за киберсигурност.

1.10. Изпълнителят трябва да разработи и имплементира набор от поне 10 оперативни сценарии (use cases) като възможни сценарии за заплахи и съответните реакции (например в случай на откриване на странично разпространение на зловреден код (lateral movement), откриване на заразени крайни точки (infected hosts), атаки за отказ от услуги (DDoS), опити за сканиране и/или нерегламентиран достъп и други).

1.11. Изпълнителят трябва да предостави План за управление на инциденти, изготвен според функционалността на продукта и способността му за управление на кибер инциденти.

1.12. Изпълнителят трябва да предостави План за тестване, описващ всички възможни оперативни сценарии, включително тестване на максимално натоварване (максимален брой събития за секунда - постоянна и пикова стойност

(sustained and peak EPS)), тестови данни, матрица на съответствието между техническите изисквания и тестовите случаи. Планът се предава, одобрява и съгласува от отговорника на проекта в „ТЕЦ Марица изток 2“ ЕАД.

1.13. Изпълнителят трябва да проведе приемните тестове на място с участието на експерти от „ТЕЦ Марица изток 2“ ЕАД.

1.14. След завършване на тестовете, Изпълнителят трябва да документира и представи резултатите от тях в доклад, който трябва да бъде одобрен и приет от Ръководителя на проекта от страна на „ТЕЦ Марица изток 2“ ЕАД. Ако ръководителят на проекта от страна на „ТЕЦ Марица изток 2” ЕАД установи, че тестовете са извършени в непълен обем спрямо тестовите процедури, той може да поиска да бъдат проведени допълнителни тестове на Системата. Резултатите от тестовете трябва да бъдат документирани и да са приложени към протокола за успешно приемане на място на системата.

1.15. Изпълнителят трябва да извършва дейностите по осигуряване на качеството съвместно с експертите на „ТЕЦ Марица изток 2“ ЕАД през целия жизнен цикъл на проекта, считано от датата на влизане в сила на договора до подписване на двустранния протокол за приключване на взаимоотношенията във връзка с гаранционните задължения на Изпълнителя.

2. Общи изисквания към оборудването и изпълнението на доставката на оборудване

2.1. Доставеното оборудване трябва да бъде оригинално, т.е. същото следва да бъде продукт на производителя на съответната марка.

2.2. Доставеното оборудване трябва да е ново, неупотребявано, в оригинални фабрични опаковки, да не е свалено от производство към датата, определена за краен срок за подаване на оферти, посочена в обявлението.

2.3. Предложеното оборудване трябва да бъде в съответствие с международните, европейските и на Република България изисквания за радиочестотни смущения, електромагнитна съвместимост, безопасност и нива на шум.

2.4. Доставеното оборудване, принадлежности и софтуер да отговорят на всички изисквания в Република България и/или ЕС относно техническа експлоатация, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

2.5. Ако законовите изисквания налагат дадено устройство или модул или принадлежност или софтуер да има лиценз за ползване, издаден от съответните контролни органи в Република България, то тези лицензи следва да бъдат представени.

2.6. Доставеното оборудване трябва да бъде окомплектовано с всички необходими силови, интерфейсни и други кабели, адаптери и аксесоари, необходими за нормалната му работа.

2.7. Захранването, силовите кабели и кабелните накрайници на силовите кабели да са предвидени за експлоатация и да отговарят на изискванията в Република България.

2.8. Всички предложени устройства да имат осигурена безплатна гаранционна поддръжка на мястото на експлоатация за период не по-къс от посочения в документацията. Гаранцията трябва да включва всички разходи (за резервни части, аксесоари, материали, труд, транспорт и т.н.) за периода на гаранционния срок.

2.9. Всички предложени устройства да са окомплектовани с необходимия хардуер, модули, кабели, софтуер, лицензи и други, така че да са работоспособни и да изпълняват функциите, заложени в техническите изисквания. Ако се окаже, че устройство не може да изпълнява дадена функция поради недостиг или липса на хардуерен модул, софтуер или лиценз, то съответните елементи трябва да бъдат доставени безплатно.

2.10. Предложените комуникатори, маршрутизатори и сървъри да имат включена безплатна софтуерна поддръжка на системния софтуер (BIOS, firmware, драйвери и т.н.) за период не по-къс от посочения в документацията гаранционен срок. Тази поддръжка да е свободно достъпна за оторизирани представители на Възложителя от интернет сайта на производителя. Интернет сайтът да поддържа версия на български и/или английски език.

2.11. В случай на спиране на производството на предлаганото оборудване по време на провеждане на обществената поръчка, поради внедряване на нови технологии, трябва да се предложи оборудване със същите или по-добри характеристики от актуалната продуктова листа на съответния производител.

2.12. Устройствата да могат да се монтират в комуникационен шкаф и към тях да бъдат включени всички необходими елементи за монтаж. Не се допуска монтиране върху „тава”.

2.13. Комуникационните шкафове, в които ще се монтира оборудването са стандартни - 42 U / 600 [mm] / 1000 [mm].

2.14. Предложеното компютърно оборудване трябва напълно да отговаря на изискванията, заложени в техническите изисквания.

2.15. Оборудването и прилежащите към него софтуер, периферни устройства и други модули и аксесоари, необходими за правилното му функциониране, следва да бъдат доставени на адрес, посочен от Възложителя и в ден, предварително уговорен с Възложителя.

3. Гаранционни изисквания

3.1. Изпълнителят трябва да осигури гаранционна техническа поддръжка за не по-малко от 12 месеца за цялата Система (хардуерни и софтуерни компоненти).

3.2. Изпълнителят трябва да предостави софтуерните лицензи с включена поддръжка за не по-малко от 36 месеца.

3.3. Техническа поддръжка трябва да бъде достъпна по телефона, чрез електронна поща и/или уеб интерфейс 24 x 7.

3.4. Поддръжката трябва да включва софтуерни актуализации и надстройки, корекции на грешки, и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение.

3.5. Времето за отстраняване на възникнали проблеми и/или подмяна на неработещи модули е не повече от 48 часа.

3.6. Ако повреда на хардуера не може да бъде отстранена на място, ремонтът се извършва в оторизиран от производителя сервиз.

3.7. Ако повредата не може да бъде отстранена в рамките на 48 часа, Изпълнителят следва да предостави на Възложителя за времето на отстраняване на повредата оборотно оборудване от същия функционален тип.

3.8. При невъзможност за отстраняване на повредата, отказалият хардуерен компонент трябва да се замени.

3.9. Компонентите на решението трябва да бъдат доставени от Изпълнителя.

3.10. Разходите за замяна или ремонт, за всички компоненти на Системата, както и всички други разходи за изпълнение на гаранционните задължения на място, включително за труд и транспорт, са за сметка на изпълнителя, ако се дължат на фабрични дефекти, на изпълнението на инсталационни и конфигурационни дейности и не са предизвикани от неправилна експлоатация.

3.11. Гаранционният срок на предмета на поръчката започва да тече от датата на протокола на успешно проведени 72-часови проби.

3.12. След внедряване на продукта, Изпълнителят се задължава да осигури допълнително съдействие за срок от 3 месеца за фино донастройване на функционалните параметрите на Системата и допълване на оперативни сценарии за работа (use cases).

4. Изисквания, свързани с обучението

4.1. Обучението е предназначено за технически специалисти на „ТЕЦ Марица изток 2“ ЕАД, които впоследствие ще извършват техническо обслужване и отстраняване на откази на доставеното Оборудване (хардуер и софтуер) както и за аналитици по сигурността.

4.2. Обучението трябва да бъде проведено от квалифицирани инструктори, оторизирани от фирмата производител на Системата.

4.3. Изпълнителят трябва да осигури обучение за предложените продукти за предложените от централата специалисти. Обучението трябва да включва, но не се ограничава до:

4.3.1. Принципа на работа, техническите характеристики, блоково-функционалната схема, функциите на съставните части и процесите при тяхното взаимодействие, предоставяните услуги, както и конфигурационните параметри на всяка функция, услуга и хардуерен компонент;

4.3.2. Функционалността на модула за управление на инциденти (ескалиране, проследяване, разрешаване);

4.3.3. Управление на правата за достъп;

4.3.4. Извършване на диагностика и локализиране на откази до ниво модул с използване на средствата за управление и посредством отчитане на локалните индикатори;

4.3.5. Да възстановяват работоспособността на Системата с използване на модули, за чиято подмяна в експлоатационни условия е налична инструкция от производителя на Системата и тя е включена в доставената документация;

4.3.6. Да инсталират, да конфигурират, обновяват, надграждат и поддържат в работоспособно състояние софтуера;

4.3.7. Да извършват архивиране и възстановяване от архив на конфигурационните параметри.

4.4. Изпълнителят трябва да осигури обучение за предложените продукти за аналитици по сигурността. Обучението трябва да включва, но не се ограничава до:

4.4.1. Да добавят нови информационни активи към базата данни от мониторирани активи;

4.4.2. Да разчитат и анализират регистрираните записи на събития/инциденти и да ги категоризират по зададени критерии;

4.4.3. Да извършват разследване на инциденти като използват всички налични модули и функционалности на Системата;

4.4.4. Да усвоят задълженията на аналитиците по сигурност от първо и второ ниво и как те си взаимодействат, използвайки функционалностите на Системата;

4.4.5. Да усвоят как да зареждат и използват информация от достъпните външни канали за актуалните кибер-заплахи (threat intelligence feeds);

4.4.6. Да работят с: маскирани данни; създаване и вадене на справки; функционалността на модула за управление на инциденти (ескалиране, проследяване, разрешаване); оперативни сценарии за работа (Use cases).

4.5. Изпълнителят трябва да представи план за обучение, преди провеждане на обучението, който трябва да бъде одобрен от Ръководителя на проекта в „ТЕЦ Марица изток 2“ ЕАД.

4.6. Изпълнителят трябва да осигури учебни материали за обучението.

4.7. Изпълнителят трябва да предостави Ръководства за потребителя за предложените продукти.

4.8. Изпълнителят трябва да предостави технически ръководства за предложените продукти.

4.9. Успешно преминалите обучението участници трябва да получат документ, удостоверяващ този факт.

5. Регулаторни изисквания

5.1. Решението трябва да бъде в съответствие с изискванията на индустриалните стандарти и европейските регламенти.

5.2. Решението трябва да подпомага реализацията, поддръжката и подобряването на Системата за управление на информационната сигурност в

„ТЕЦ Марица изток 2“ ЕАД, базирана на стандарта ISO/IEC 27001, в частта технически механизми за контрол.

5.3. Изпълнителят трябва да приложи процес на разработка и свързаните с него дейности, резултати и продукти в съответствие с изискванията на общоприетите и доказани международни стандарти в индустрията (IEEE / EIA, ISO / IEC).

6. Изисквания по безопасност

Софтуерът трябва да бъде разработен с ниво на сигурност на програмното осигуряване 4 (SWAL4), (изключвайки целите, свързани с безопасността).

7. Изисквания по информационна сигурност

7.1. Системата трябва да поддържа сигурна комуникация между всички нейни модули, чрез използване на криптирани канали между отделните компоненти.

7.2. Системата трябва да притежава опция за повишаване на сигурността (hardening) в съответствие с STIG (Security Technical Implementation Guide).

7.3. Системата трябва да поддържа като минимум следните правила за сложност на пароли:

7.3.1. Минимална дължина на паролата;

7.3.2. Минимален брой главни букви;

7.3.3. Минимален брой малки букви;

7.3.4. Минимален брой десетични цифри (от 0 до 9);

7.3.5. Минимален брой специални символи;

7.3.6. Дали паролата може да съдържа потребителско име или не;

7.3.7. Потребителят да може да промени своята парола при първи вход в Системата.

7.4. Системата трябва да позволява промяна на първоначалната парола на системния администратор (admin, root).

7.5. Решението трябва да поддържа като минимум следните системни настройки за сигурност:

7.5.1. Период на заключване;

7.5.2. Период на неактивност;

7.5.3. Време за изтичане на сесия;

7.5.4. Потребителски имена, нечувствителни към главни/малки букви;

7.5.5. Максимален допустим брой неуспешни опити за вход в Системата;

7.5.6. Период на валидност на потребителските пароли за цялото Оборудване;

7.5.7. Уведомяване на потребителите <n> дни преди изтичане на срока на валидност на паролите.

7.6. Системата трябва да поддържа персонализиран банер, изискващ от потребителите да се съгласят с условията преди да влязат в Системата.

7.7. Решението трябва да позволява налагането на принципите „Разделяне на правата” и „Принцип на минималните права (принцип на максималните ограничения)”.

7.8. Решението трябва да предоставя възможност за реализация на механизми за идентификация и автентикация, които да ограничат достъпа до определен тип данни.

7.9. Изпълнителят трябва да обезпечи сигурността на чувствителната информация по време на пълния жизнен цикъл (например: транспорт, съхранение, одит, архив, бекъп, изтриване).

7.10. Защитните стени, заедно с прилежащия им софтуер, трябва да притежават сертификат Common Criteria Evaluation Assurance Level (EAL) 4+ или по-висок.

Специфичният софтуер за проследяване на активността на IT средата на предприятието или еквивалент. Софтуерът идентифицира и категоризира инциденти и събития като ги анализира. Предоставя отчети за инциденти и събития, както и изпраща предупреждения за потенциални проблеми, свързани със сигурността.

8. Специфични условия и изисквания към изпълнението

8.1. Системите следва да са окомплектовани с кратко описание и/или техническа документация на български език и/или английски език и инструкции за експлоатация на български език и/или английски език.

8.2. При инсталиране и конфигуриране на Системите, следва да се използват методика, практики и процедури, препоръчани от производителя на съответното оборудване.

8.3. Системите следва да се интегрират в съществуващата инфраструктура на Възложителя.

8.4. Изпълнителят следва да предложи схема за приемане на заявки и реакция при възникване на проблеми: изградени help-desk система и/или единен сервизен телефонен номер за получаване и обработка на заявките при възникване на проблеми и да посочи лице за контакт.

9. Изисквания към преработването на съществуващите компютърни мрежи и изграждане на три нови компютърни мрежи: „Производствена”, „Административна” (съставена от две отделни части с различни функционални характеристики) и „Публична” компютърна мрежа

С оглед на по-горе изложеното и с цел осигуряване на киберзащита на компютърните мрежи (информационните системи) на професионално ниво е необходимо да бъдат преработени съществуващите компютърни мрежи и да бъдат изградени 3 нови компютърни мрежи: „Производствена”, „Административна” (съставена от две отделни части с различни функционални характеристики) и „Публична” компютърна мрежа.

9.1. Специфика и предназначение на новоизградените компютърни мрежи

9.1.1. Производствена компютърна мрежа

Тази компютърна мрежа ще обхваща всички персонални компютри и други електронни устройства, които са включени в управлението на производствения процес (производството на електрическа енергия).

Това е мрежа от затворен (закрит) тип. Задължително тази мрежа и всичките включени в нея устройства нямат връзка с интернет.

Компютърната мрежа трябва да използва само оптичен кабел за връзка между отделните устройства.

Тази мрежа може да включва отделни електронни устройства, които имат свободни портове за връзка с други устройства, но ползването на тези портове трябва да бъде само от лица със специални разрешения и с устройства, за които е доказано, че са „чисти".

Защитата от хакерски атаки за тази компютърна мрежа следва да бъде от най-висок клас.

9.1.2. Административна компютърна мрежа

Тази компютърна мрежа обхваща всички персонални компютри и други електронни устройства, които се използват в административната дейност на централата (създаване на различни документи и техния обмен).

Компютърната мрежа трябва да използва само оптичен кабел за връзка между отделните комуникационни устройства, от които е изградена.

Тази мрежа може да включва отделни електронни устройства, които имат свободни портове за връзка с други устройства, но ползването на тези портове трябва да бъде само от лица със специални разрешения и с устройства, за които е доказано, че са „чисти".

Тази компютърна мрежа ще включва две отделни части, които ще са отделени една от друга със съответните подходящи хардуерни устройства и софтуер.

Първата част ще е от затворен (закрит) тип и обслужва вътрешната административна дейност на централата. Задължително тази част от мрежата и всичките включени в нея устройства нямат никаква връзка с интернет.

Втората част ще е от отворен (публичен) тип (корпоративна) и ще обхваща информационните потоци (приемане, изпращане и обмен) между администрацията на централата и външни лица и структури. Тази част от мрежата и включените в нея устройства ще имат връзка с интернет. Достъпът на външните лица и структури до тази мрежа следва да се разрешава само след като те се идентифицират с име и e-mail адрес.

Защитата от хакерски атаки за тази компютърна мрежа следва да бъде от висок клас.

9.1.3. Публична компютърна мрежа

Тази компютърна мрежа ще създава средата за собствените персонални електронни устройства на работещите и гостите на територията на „ТЕЦ Марица изток 2" ЕАД.

Тази мрежа ще е изцяло публична и включените в нея устройства ще имат връзка с интернет.

Компютърната мрежа може да използва оптичен кабел и медни проводници с изводи на определени места за свободно включване и достъп. Същевременно, тази мрежа трябва да осигурява стабилна Wi - Fi връзка с интернет и между отделните устройства.

Особеност на тази мрежа е, че тя ще работи само с крайни устройства, които не са собственост на „ТЕЦ Марица изток 2" ЕАД.

Защитата от хакерски атаки за тази компютърна мрежа следва да бъде от среден клас.

За обезпечаване работата на компютърните мрежи (информационните системи) в „ТЕЦ Марица изток 2" ЕАД е необходимо да се изгради високоскоростна комуникационна LAN мрежа, която да обхваща цялата територия на „ТЕЦ Марица изток 2" ЕАД. Комуникационната LAN мрежа трябва да бъде съобразена със съществуващата кабелна (оптична и медна) инфраструктура. При необходимост е допустимо изграждането на допълнителна кабелна инфраструктура, която изрично трябва да бъде съгласувана и одобрена от Възложителя. Топологията на комуникационната LAN мрежа трябва да бъде логически тип „звезда", като трафика от всеки отдалечен комуникационен възел трябва да се терминира в централните опорни комутатори.

От съображение за сигурност и висока надеждност е необходимо да се обособят основен и резервен център за съхранение на данни, които се явяват и основни комуникационни възли за локалната LAN мрежа. Основният Data Center трябва да се изгради в Главната административната сграда, а резервния Data Center в скривалището.

Централният комуникационен възел трябва да се обособи в точката, където физически са съсредоточени всички оптични кабели, свързващи отдалечените комуникационни възли, в който да се инсталират опорните комутатори на локалната мрежа LAN. Към него, посредством оптична инфраструктура на територията на „ТЕЦ Марица изток 2" ЕАД, ще се свързват новоизградени опорни комуникационни възела в следните сгради:

- Административни сгради;
- Портали - 6 броя;
- Столова (на 500 [m]);
- Кафенета - 4 броя;
- Магазин;
- Медицински център;
- Сграда „Охрана";
- Блочни щитове за управление - 4 броя;
- Складове - 12 броя;
- Помпени станции - 3бр.

Комуникационните LAN връзки между основния Data Center и опорните комуникационни възли трябва да бъдат резервирани и да осигуряват скорост за предаване на данни минимум 1 GBps.

9.2. Минимални технически изисквания към мрежовото оборудване за изграждане на опорна комуникационна мрежа

Минимални технически изисквания към мрежовото оборудване за изграждане на опорна комуникационна мрежа в централния комуникационен възел.

Минимални технически изисквания към управляем комутатор за опорната LAN мрежа:

№	параметри
1.	Тип: L3 управляем, с възможност за стекиране и монтаж в комуникационен шкаф;
2.	Маршрутизиране: RIP-1, RIP-2, RIPng;
3.	Интерфейси: минимум 24 x 10GBase-X – SFP/SFP+, минимум 1 x USB - Type A, минимум 1 x management (mini-USB) - Type B, минимум 1 x management (RS-232);
4.	Памет: минимум 4GB;
5.	Flash памет: минимум 4GB;
6.	Пропускателна способност: минимум 450 Mpps;
7.	Производителност: капацитет на комутиращата матрица минимум 640 Gbps;
8.	MAC адресна таблица: минимум 32000 entries;
9.	Протоколи за отдалечено управление: SNMP 1, SNMP 2c, SNMP 3, RMON 1, RMON 2, Telnet, SSH, CLI;
10.	Методи за удостоверяване: Secure Shell (SSH), RADIUS;
11.	Стандарти: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s;
12.	Допълнителна поддръжка: Auto-negotiation, ARP support, trunking, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, Syslog support, IPv4 support, IPv6 support, Multiple Spanning Tree Protocol (MSTP) support, DHCP snooping, Access Control List (ACL) support, Quality of Service (QoS), RADIUS support, Virtual Route Forwarding-Lite (VRF-Lite), MLD snooping, Dynamic ARP Inspection (DAI), Rapid Per-VLAN Spanning Tree Plus (PVRST+), Link Aggregation Control Protocol (LACP), layer 3 load balancing, Energy Efficient Ethernet;
13.	Капацитет: минимум 24000 IPv4 routes , минимум 48000 NetFlow entries, минимум 1000 Switched virtual interfaces (SVIs);

14.	SFP модули: минимум 1x SFP+ 10Gb с дължина на вълната 1310 nm, SMF, LC connector;
15.	Слот за разширение: минимум 1 свободен за добавяне Plug-in модул за разширение;
16.	Операционна система: Да поддържа IPv6 Routing;
17.	Стеково свързване: Съвместимо със съществуващ в университетската локалната мрежа на „ТЕЦ Марица изток 2“ ЕАД опорен комутатор Cisco WS-C3850-12S;
18.	Захранване: минимум 1 (вътрешно, с опция за допълнително захранване) и поддръжка на резервираност на захранванията (1+1);
19.	Шаси: за монтаж в шкаф с включени необходимите монтажни елементи.

Минимални технически изисквания към мрежовото оборудване за изграждане на опорни комуникационни възли за LAN достъп:

Опорните комуникационни възли трябва да бъдат изградени на подходящи места в съответните сгради, където е терминиран оптичния кабел към централния комуникационен възел. Всеки възел трябва да осигурява минимум 12 порта x 100/1000 BaseT за свързване на потребители към LAN мрежата. В точките, в които се предвижда свързване на устройства за безжичен достъп AP, трябва да се осигурят необходимия брой PoE портове за захранване.

Комуникационните LAN връзки между основния дейта център и опорните комуникационни възли трябва да бъдат резервирани и осигуряват скорост за предаване на данни минимум 1 GBps

Активното и пасивно мрежово оборудване трябва да бъдат инсталирани в подходящи комуникационни шкафове (RACK).

Минимални технически изисквания към мрежовото оборудване за изграждане на отдалечените комуникационни възли за LAN достъп:

- Да осигури минимум 24 порта 100/1000BaseT и 2 порта 1000Base LX;
- Поддръжка на IPv4, IPv6 и L2 функционалност;
- Поддръжка на протоколи: IEEE 802.1d, 802.1w, 802.1s, 802.1X, 802.3ad Link Aggregation Control Protocol (LACP), IGMP v1,v2,v3, SSH v1,v2 и SSL;
- поддръжка на RADIUS и TACACS автентикация;
- управление посредством SNMPv1,2c,3, RMON и CLI.

Минимални технически изисквания към управляем маршрутизатор:

№	параметри
1.	Маршрутизаторът трябва да е модулен, което да позволява бъдещо разширяване на броя интерфейси;
2.	Маршрутизаторът трябва да притежава фабрично вграден криптиращ ускорител;

3.	Маршрутизаторът да притежава поне 2 бр. вградени Layer3 порта с възможност за предаване на данни със скорост 10/100/1000 - RJ-45 – базирани;
4.	Маршрутизаторът трябва да притежава възможност за разширяване с поне 4 допълнителни модула;
5.	Маршрутизаторът трябва да поддържа пропускателна способност минимум триста хиляди пакета за секунда;
6.	Маршрутизаторът трябва да поддържа скорост на криптиране минимум 170 Mbps;
7.	Маршрутизаторът трябва да има възможност да поддържа минимум 75 SSL/VPN тунела;
8.	Маршрутизаторът трябва да поддържа минимум 150 IPSec VPN тунела;
9.	Маршрутизаторът трябва да може да балансира трафика през паралелни пътища с различна скорост и дължина, използвайки максимално капацитета на линиите;
10.	Маршрутизаторът трябва да поддържа NAT функционалност;
11.	Маршрутизаторът трябва да терминира IPSEC тунели;
12.	Маршрутизаторът трябва да поддържа MLPPP функционалност;
13.	Маршрутизаторът трябва да поддържа Dial-backup, с автоматично преминаване от основната към резервната линия и обратно. Същата резервна линия може да бъде използвана и като спомагателна, когато натоварването на основната надхвърли определен процент;
14.	Маршрутизаторът трябва да поддържа основните VPN технологии - Access, Intranet и Extranet VPN;
15.	Маршрутизаторът трябва да поддържа MPLS-VPN и следните стандарти и препоръки - RFC 2547, RFC 2283;
16.	Маршрутизаторът трябва да поддържа MPLS-VPN в P и PE режим;
17.	Маршрутизаторът трябва да поддържа IPsec, в транспортен и тунелен режим;
18.	Маршрутизаторът трябва да поддържа различни алгоритми за криптиране и автентикация, в т.ч. DES, 3DES, AES, MD5, SHA и други;
19.	Маршрутизаторът трябва да поддържа динамични схеми за обмен на ключове (IKE);
20.	Маршрутизаторът трябва да поддържа следните стандарти и препоръки - IPsec - RFC 2401-2411, 2451;
21.	Маршрутизаторът да има вградени в операционната система възможности за защитна стена и филтриране на трафика;

22.	Маршрутизаторът да има интегриран в операционната система DHCP сървър;
23.	Маршрутизаторът трябва да поддържа WEB кеширане чрез WCCP протокол;
24.	Маршрутизаторът трябва да поддържа следните протоколи: IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN
25.	Маршрутизаторът трябва да поддържа следните енкапсулации: Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE)
26.	Маршрутизаторът трябва да притежава следните механизми за трафичен инженеринг: QoS; Class-Based Weighted Fair Queuing (CBWFQ); Weighted Random Early Detection (WRED); Hierarchical QoS; Policy-Based Routing (PBR); Performance Routing (PfR);

	Network-Based Advanced Routing (NBAR).
27.	Маршрутизаторът трябва да притежава слените протоколи за мрежово наблюдение и управление: SNMP; Remote Monitoring (RMON); syslog; NetFlow.
28.	Захранване шуко - 240AC;
29.	Маршрутизаторът трябва да бъде монтиран в 19" комуникационен шкаф.

9.3. Минимални технически изисквания към изграждането на открита LAN мрежа за безжичен достъп до Интернет („Публична компютърна мрежа”)

На територията на централата е необходимо да бъде изградена високоскоростна безжична комуникационна мрежа за публичен достъп до Интернет в следните основни точки:

- Административна сграда - 4 етажа;
- Портали - 6 броя;
- Столова (500 м^2);
- Кафе;
- Магазин;
- Медицински център;
- Охрана;
- Резервна точка.

Безжичната комуникационна мрежа трябва да отговаря на последните стандарти за изграждане на безжични мрежи, като осигурява високоскоростен контролиран достъп до Интернет на всякакъв вид мобилни устройства.

Свързването към безжичната мрежа да се осъществява с помощта на потребителско име и парола.

Минимални технически изисквания към контролера за управление на безжичен достъп (AP) - основен и резервен:

- Минимум 4 dual-media порта (1000BASE-X or 10/100/1000BASE-T);
- Минимум 2 10 GBASE-X порта;
- Минимум 2 USB 2.0 порта;
- Контролерът трябва да управлява минимум 250 крайни точки;
- Да има възможност за създаване на минимум 4000 VLANs;
- Минимум 4000 едновременни SSL сесии;
- Минимум 12 Gbps безжична пропускателна способност;
- Контролерът да има LCD panel и бутони за навигация;
- Контролерът трябва да предлага графичен/уеб интерфейс за управление, мониторинг и диагностика на безжичната мрежа;
- диагностика на безжичната мрежа;
- Идентификация на трафика от и към различните приложения;

•Контролерът трябва да поддържа архитектурните сценарии за bridge, bypass и inline архитектури;

•Контролерът трябва да поддържа автентикация на потребителите през портал;

•Трябва да има възможност за ребалансиране на потребителите между няколко точки за достъп;

•Възможност за калибриране и рекалибриране на сигнала на ТД (точки за достъп) с цел да се постигне най -добър сигнал спрямо външни съобщения и съседните ТД.

Минимални технически изисквания към устройства за безжичен LAN достъп:

•Предложеното устройство да бъде управлявано и съвместимо с предложения контролер;

•Предложеното устройство да поддържа 802.11a/b/g/n/ac;

•Предложеното устройство да притежава USB 2.0 interface;

•Предложеното устройство да притежава минимум един 10/100/1000BASE-T Ethernet network interfaces (RJ-45);

•Предложеното устройство да бъде предназначено за вътрешен монтаж;

•Да поддържа Dual Radio, 5 GHz 802.11ac 4x4 MIMO и 2.4 GHz 802.11n 2x2 MIMO;

•Вграден Bluetooth Low-Energy (BLE);

•Производителност минимум 1700 Mbps при 5 GHz band и минимум 300 Mbps при 2.4 GHz band;

•Устройството да придружено с всички необходими лицензи и планки за монтаж;

•Да поддържа PoE;

•Да има възможност за Stand-alone управление, управление чрез контролер и чрез Cloud приложение;

•Максималната консумация на енергия да не надхвърля 15W;

•Да предоставя възможност за видимост и контрол върху приложенията;

•Да поддържа технология за автоматично назначаване на радио канали и мощност;

•Да предотвратява интерференцията с цел максимална производителност на мрежата;

•Да има възможност за проследяване на локация и навигация на клиентите.

9.4. Минимални технически изисквания към преобразуване на съществуващите персонални компютри във виртуални работни станции (терминали)

Съществуващите персонални компютри следва да бъдат преобразувани във виртуални работни станции, като се изпълнят следните условия:

•Доставка на необходимия хардуер и софтуер за виртуализация и управление на минимум 400 броя виртуални работни станции с Windows операционни системи;

•Да позволява интеграция с облачни услуги;

•Да е от производителя на виртуализационния софтуер за сървърите, с цел интегрирано управление;

•Да осигурява необходимия брой лицензи съобразно броя на работните станции.

10. Изисквания за изграждане на клъстерна сървърна система, състояща се от 4 основни и 4 резервни виртуални сървъра. Апликации и архивиране на информацията в основния и резервния Data Center

10.1. Минимални изисквания за изграждане на клъстерна сървърна система, състояща се от основни и резервни виртуални сървъри.

За обезпечаване на системите за обработка и съхранение на данни е необходимо да се изградят основна и резервна сървърни системи за обработка и съхранение на информацията.

Основната сървърна система се инсталира в основния Data Center, а резервната сървърна система се инсталира в резервния Data Center.

Сървърните системи трябва да осигуряват резервираност, да работят в клъстер и посредством виртуализация да осигуряват по минимум 4 сървъра във всеки един Data Center (общо 8 сървъра).

Във всеки един Data Center трябва да бъдат инсталирани минимум 2 (две) физически сървърни машини и минимум един сторидж.

С оглед безотказната работа в режим 24 х 7 и обезпечаване на необходимия трансфер на данни между сървърните системи и системите за съхранение на информацията (сторидж), между двата Data Center трябва да бъде изградена високоскоростна LAN / SAN резервирана комуникационна мрежа със скорост на връзките минимум 40 GB/s.

10.2. Минимални технически изисквания към оборудването за изграждане на клъстерна сървърна система, състояща се от основни и резервни виртуални сървъри.

10.2.1. Сървърно оборудване и софтуер

№	сървърно оборудване и софтуер	технически изисквания
1.	Шаси	Минимум 2U с релси за монтиране в шкаф.
2.	Процесор	Минимум 2 броя Intel Xeon Gold 6130 16C 125 W 2,1 GHz или еквивалентни.
3.	Памет	Минимум 16 броя 32 GB TruDDR4 2666 MHz RDIMM;
		Да има минимум 24 DIMM слота за възможност за разширение;
		Да поддържа минимум RDIMMs, LRDIMMs или 3DS RDIMMs;
		Скорост на памет минимум 2666 MHz.

4.	Дискова система	Възможност за инсталиране на минимум 8 броя 2.5“ SAS/SAT HDD;
		Инсталиран хардуерен RAID controller 12 Gb SAS с поддържани нива 0, 1, 10, 5, 50.
5.	Разширителни портове	Да има минимум:
		1 брой двупортова 10 GbE SFP+ ports (no 10/100 Mb support) с включени минимум 2 броя Passive DAC SFP+ Cable;
		1 брой четирипортова 1Gb RJ45 Ethernet Adapter;
		1 брой RJ-45 10/100/1000 Mb Ethernet management port.
		Възможност да се разширява до минимум 7 PCIe слота.
6.	Други интерфейси	Преден панел минимум:
		1 брой USB 2.0 port;
		1 брой USB 3.0 port;
		Възможност за добавяне на 1 брой DB-15 VGA порт.
		Заден панел минимум:
		2 броя USB 3.0;
		1 брой DB-15 VGA;
		Възможност за 1 брой DB-9 сериен порт.
7.	Захранване	Минимум 2 броя захранващи Hot-Swap блока с минимум 1000 W мощност.
8.	Hot-swap елементи	HDD;
		Захранващи блокове;
		Вентилатори.
9.	Инсталирани ОС	Минимум 2 броя Windows Svr 2016 Standard (16 core) за сървър.
10.	Поддържани ОС	Microsoft Windows Server 2012 R2 and 2016;
		Red Hat Enterprise Linux 6 (x64) and 7;
		SUSE Linux Enterprise Server 11 (x64) and 12;
		VMware vSphere (ESXi) 6.0 and 6.5.
11.	Гаранционен срок	Една година на място при клиента с ниво на поддръжка 24/7 с гарантирано време за отстраняване на повредата до 24 часа след повдигане на сервизна заявка и без да се връщат компоненти, на които се съхранява информация на клиента
12.	Софтуер за виртуализация	Да позволява инсталация на хипервайзор директно върху хардуера;

		Поддръжка на поне 528 логически процесора, предоставени от хардуера;
		Поддръжка на поне 1000 виртуални машини;
		Поддръжка на преместване на работеща виртуална машина от един сървър на друг;
		Поддръжка на преместване на работеща виртуална машина от един дисков масив на друг;
		Поддръжка на различни „гост“ операционни системи, като Windows, Linux, BSD;
		Да се доставят необходимите лицензи за виртуализационен софтуер за 2 сървъра с по 2 процесора, както и необходимите лицензи за управление на тази инфраструктура;
		Да има включен 3 годишен абонамент и поддръжка.

10.2.2. Система за съхранение на информацията (Storage system)

- Блок сториджс, позволяващ достъп до данните по Fibre channel, iSCSI/FCoE и SAS интерфейси включително и едновременно;
- Двоен контролер, гарантиращ непрекъснатост на достъпа до данните;
- Поддържани брой дискове - Минимум 700 броя;
- Поддръжка на дву-портови дискове с автоматично засичане на проблем;
- Разширителни шасита - да събират мин. 64 диска SSD, NL SAS, SAS;
- Захранване - Резервирано;
- Възможност за подмяна на дефектирали захранвания, вентилатори и дискове без спиране на работата на сториджа;
- Поддържани RAID нива – 0/1/10/5/6;
- Поддържани дискове: SAS, NL SAS, SSD 2,5“ и 3.5“:

✓ 400GB, 800GB, 1.6TB, 3.2TB, 3.8TB, 1.9TB, 7.6TB, 15.3TB SAS3 SSDs;
✓ 300GB, 600GB и 900GB 15K rpm SAS HDDs;
✓ 900GB, 1.2 TB, 1.8 TB, 2.4 TB 10K rpm SAS HDDs;
✓ 2 TB 7.2K rpm NL SAS HDDs;
✓ 4TB, 6TB, 8TB, 10TB 7.2K rpm NL SAS HDDs;

- Памет на контролер: мин. 32 GB, защитена с батерия;
- Включени функционалности:

✓ Frontend свързаност: 8x16Gb FC, 2x10 Gb iSCSI;
✓ Инсталирани дискове:

- Минимум 4x 400GB SSD;
- Минимум 20 x 1.2TB 10,000 rpm 12 Gb;
- Минимум 12 x 10TB 7.2к

✓ Софтуер (прилежащ софтуер за управление на дисковия масив): Включени лицензи:

- Виртуализация на вътрешното пространство;
- Tiering - автоматичен;

- Inline компресия на данните;
- Двупосочна репликация на данни, синхронно или асинхронно;
- Моментни копия (snapshots), пълни копия (clone).

10.2.3. Активно оборудване за изграждане на LAN / SAN сървърна мрежа (за основен и резервен Data Center)

- Комутаторът трябва да е специализирано мрежово устройство с височина 1U, подходящо за монтиране в комуникационен шкаф;
- Комутаторът трябва да има не по-малко от 32 порта, предназначени за модули с 40-гигабитови Ethernet QSFP+;
- Устройството трябва да поддържа QSFP+ 40 Gigabit Ethernet модули, не по-малко от SR и медни модули (Direct Attach Copper);
- Комутаторът трябва да поддържа най-малко следните разширителни модули:
  - ✓ 10GbE QSFP+: 100 (with breakout cable);
  - ✓ 40GbE QSFP+: 30;
  - ✓ 100GbE QSFP28: 4.
- Трябва да е възможно да преобразувате всеки 40-гигабитен Ethernet порт на 4 10-гигабитови Ethernet портове;
- Устройството трябва да поддържа SFP + 10 Gigabit Ethernet модули минимум SR, USR, LR, ER, ZR. В допълнение, устройството трябва да поддържа медни модули (Direct Attach Copper) за 10 Gigabit Ethernet и 40-гигабитови Ethernet връзки;
- Устройството трябва да поддържа SFP модули минимум LH, LX, SX и Base-T;
- Устройството трябва да има сменяем вентилационен модул;
- Устройството трябва да има най-малко 2 броя порта за управление (2x SFP fiber ports или 1x RJ-45 и 1x copper SFP ports);
- Устройството трябва да позволява работа в споделена архитектура от поне 20 комутатора, които да функционират като едно логическо устройство. Лиценз за работа в горе посоченото режим не се изисква. Ако по-горе функцията изисква допълнителни лицензи или модули, моля, предоставете ги заедно с превключвателя;
- Устройството трябва да е снабдено с поне 16 GB RAM и SSD с капацитет не по-малък от 64 GB;
- Управлението на устройствата трябва да се осъществява чрез интерфейса на командния ред (CLI) през конзолния порт, telnet, ssh;
- Агрегираната ефективност на трансфера в Layer 2 не може да бъде по-ниска от 2,5 Tbps. Устройството трябва да поддържа не по-малко от 1,3 Bpps;
- Комутаторът трябва да поддържа VLAN, отговарящи на IEEE 802.1q, в количество не по-малко от 4000;
- Устройството трябва да поддържа обединяване на връзките в съответствие с IEEE 802.3ad - не по-малко от 128 групи за LAG;
- Комутаторът трябва да поддържа Spanning Tree Protocol и протокола Rapid Spannig Tree в съответствие с IEEE 802.1D- 2004, както и Multiple Spanning Tree в съответствие с IEEE 802.1Q-2003;

- Устройството трябва да поддържа маршрутизиране между протоколите VLAN - статично маршрутизиране и динамично маршрутизиране: RIP, OSPF. Трябва да има възможно за разширение за използване на протоколи IS-IS и BGP. Комутаторът трябва да може да обработва 120 000 префикси по хардуер и поне 280,000 MAC адреси;
- Устройството трябва да поддържа протоколи за маршрутизиране на множествено предаване, минимум IGMP (v1, v2, v3), PIM-SM и MSDP;
- Устройството трябва да има механизми за приоритизиране и управление на мрежовия трафик (QoS) в слоевете 2 и 3 за входящия и изходящия трафик . Класирането на трафика трябва да се извършва в зависимост от поне: интерфейс тип Ethernet, VLAN, приоритет на слой 2 (802.1p), MAC адреси, IP адреси, стойности на полета ToS / DSCP в IP заглавията, TCP и UDP портове;
- Комутаторът трябва да поддържа филтрация на MAC адреси;
- Устройството трябва да поддържа протокола SNMP (v1,v2,v3);
- Устройството трябва да поддържа протокола OpenFlow 1.3 и да използва приставката за OpenStack Neutron;
- Да има възможности за автоматизация с поддръжка на Python и zero touch provisioning (ZTP);
- Архитектурата на операционната система на устройството трябва да има модулна конструкция (отделните модули трябва да работят в отделни зони на паметта), включително модулът за препращане на пакети, отговорен за комутирането на пакети, трябва да бъде отделен от модула за маршрутизиране на IP, който е отговорен за установяването на маршрути за маршрутизиране и управление на устройствата;
- Устройството трябва да има механизъм за бързо възстановяване на системата и възстановяване на конфигурацията. Не по-малко от 10 предишни пълни конфигурации трябва да се съхраняват в устройството;
- С устройството се изисква да се предоставят технически грижи, валидни за определен период от 12 месеца. Поддръжката трябва да включва: техническа поддръжка, предоставена по телефона и електронна поща от производителя и Български дистрибутор на оборудване, подмяна на повреденото оборудване в рамките на следващия работен ден, достъп до нови версии на софтуера, както и достъп до бази данни, ръководства за конфигуриране и диагностични инструменти.

11. Изграждане на система за киберсигурност

Главната цел на системата за киберсигурност е да създаде необходимите правила, чието прилагане ще гарантира възможната максимална степен на защита на информацията, която се създава, пренася (обменя) и съхранява в компютърните мрежи на централата.

Основни цели на системата за киберсигурност:

- Структуриране на видовете заплахи и типовете уязвимост за използваните компютърни мрежи (информационни системи);
- Осигуряване на необходимата конфиденциалност за информацията в компютърните мрежи;

- Създаване на условия за поддържане целостта на използваната информация, както и на възможности за нейното възстановяване;
- Обезпечаване на достъп до информацията в компютърните мрежи за разрешените потребители.

11.1. Минимални технически изисквания към защитните стени

Функционалност на резервирана система от тип Интернет достъп „защитна стена”:

- Обособяване на зони с различна степен на доверие, като разделя мрежата на отделни сегменти според функционалните им характеристики;
- Обособяване на зони за комуникация с външна мрежа и контролира достъпа до тях;
- Обособяване на сървърни зони, в които се публикуват вътрешните услуги. Контролира трафика между тези зони и всички външни такива;
- Контролира трафика между зоните с вътрешни потребители и Интернет;
- На база на акредитация от Активната Директория контролира поведението на всеки един потребител при достъпа му до Интернет и вътрешните ресурси.
- Инспекция на трафика и идентификация на приложенията;
- Защита от мрежови атаки чрез система за превенция на атаките (IPS);
- Системата да анализ на съдържанието за наличие на зловреден код (AntiVirus и AntiSpyware);
- Системата да анализира Zero Day на зловреден код чрез стартиране на файла във защитената среда;
- Филтриране на уеб сайтовете по категории с цел да се ограничи достъпа на потребителите на вътрешни за мрежа до ресурси до опасно съдържание в Интернет;
- Наличие на DLP (Data Loss Prevention) функционалност, като по този начин ще се осъществява идентификация на файлове по име и разширение, изпращани и/или получавани в мрежовия трафик, за да се минимизира възможността за изнасяне на конфиденциална информация и контрол на информационните канали;
- Инспекция на HTTPS протокола - декриптиране и инспекция на входяща и изходящ SSL мрежова комуникация;
- Декриптиране на SSL мрежова комуникация, която транспортира в себе си криптирани SMTP, IMAP, POP3, FTP и пр.;
- Декриптирането на SSL трафика, прозрачно за всички функционални компоненти на системата: IPS, AntiVirus, AntiSpyware, инспекция на данни и файлове, и URL филтриране;
- Блокиране на всички приложения чрез прилагане на принципа за минималния достъп (The Principle of Least Privileges) - всички приложения, които не са изрично указани като разрешени за използване в конфигурираните в системата политики, да бъдат блокирани;
- Идентификация на приложенията без оглед на използвания от тях комуникационен порт, протокол (включително P2P, IM, Skype, Webmail, Webex

и пр.) и криптирана или не форма на комуникация с цел налагане на политики и спазване на правилата за информационна сигурност;

- Възможност за конфигурация на политиките за сигурност чрез дефиниране на източника на мрежовата комуникация, крайната цел на мрежовата комуникация (посока), приложението и/или приложенията, за които се отнася политиката, дефиниране на мрежовите услуги както и каква да бъде активната реакция ако критериите бъдат изпълнени;
- Препращане на подозрителните DNS заявки към специално подбран произволен адрес с цел бърза идентификация и блокиране на комуникацията на заразени хостове от вътрешната мрежа (DNS sinkholing);
- Механизъм, интегриран в мениджмънт интерфейса, който да позволява корелация между аномалиите в мрежовия трафик и поведението на крайните потребители с цел идентификация на потенциално заразени крайни станции, които са част от ботнет мрежи;
- Възможност за дефиниране на VLAN-и за Layer 2 и Layer 3 интерфейсите с цел да се осигурят гъвкави механизми за инспекция на трафика, които да поддържат създадените за нуждите на организацията мрежови сегменти;
- Възможност за изграждане на site-to-site VPN тунели на база IPSec и IKE стандартите. Приложение на SSL стандарта за реализация на client-to-site топология за предоставяне на сигурен криптиран достъп до централизираните информационни ресурси;
- Възможност за управление и приоритизиране на трафика (QoS) според типа приложение;
- Прозрачна идентификация на потребителите без изискване да се предоставят потребителско име и парола;
- Възможност за дефиниране на индивидуални маршрутизиращи таблици с цел осигуряване на маршрутизиращи функционалности за различните мрежови сегменти;
- Възможност за конфигурация на две устройства да работят в режим на отказоустойчивост (High-availability), чрез конфигуриране Active-Active или Active-Passive клъстер;
- Възможност за мониторинг, анализ на логовете и репортинг от самото устройство;
- Уеб базиран интерфейс за управление на устройството и индивидуално дефинируеми в системата полета за показване на различни статистики на база време, приложение, категории, потребители, заплахи и пр.;
- С цел адекватен мениджмънт и генериране на специално създадени за целта доклади, показващи нивото на сигурността в „ТЕЦ Марица изток 2“ ЕАД и трафика към Интернет;
- Логовете на устройството да са достъпни в уеб интерфейса с възможност за контекстуално филтриране или филтриране на база ключова дума. Информацията следва да е обогатена контекстуално с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и др.);
- Възможност за интегриране с централизирана мениджмънт система, с която да могат да се прилагат предварително конфигурирани политики.

ПАРАМЕТЪР	МИНИМАЛНА СТОЙНОСТ
Минимална пропускателна способност	4 Gbps
Минимална пропускателна способност с активирана функция за идентификация на приложенията	4 Gbps
Минимална пропускателна способност с активирани функционалности за IPS/AntiVirus/ AntiMalware защита, URL филтриране и идентификация на файлове и чувствително съдържание в трафика	2 Gbps
Идентификация на приложенията	Функционалността следва да се осигурява от самата защитна стена
Брой TCP сесии	500,000
Брой нови сесии в секунда	50,000
Минимален брой интерфейси	12 x 10/100/1000 Base-T ports; 8 x 1000Base-X SFP ports.
Режими на интерфейсите	L2, L3, Tap, Virtual Wire (transparent mode)
Маршрутизиращи функции	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding; Point-to-Point Protocol over Ethernet (PPPoE); Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 Bidirectional Forwarding Detection (BFD).
Минимален брой VPN тунели/тунелни интерфейса	2000 IPSec VPN тунела / тунелни интерфейса
Минимални изисквания към IPSec имплементацията	Key Exchange: Manual key, IKE v1 (Pre-shared key, certificate-based authentication); Encryption: 3DES, AES (128-bit, 192-bit, 256-bit); Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512.
Минимален брой конкурентни SSL VPN потребителя включени в системата	2000 SSL VPN потребителя

Минимален брой виртуални рутери, поддържащи отделни, рутиращи таблици	10
Минимален брой поддържани VLAN	4,094 броя IEEE 802.1q VLAN маркера (tags), конфигурируеми за всеки интерфейс и общо за устройството
IPv6 поддръжка	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
Инспекция на SSL криптиран трафик трафика, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието	Системата следва да декриптира и инспектира SSL
Споделяне на декриптирания SSL трафик	Системата следва да предоставя възможност декриптирания SSL трафик да може да бъде споделян през mirror port с други системи, които не разполагат с възможност за декриптиране на SSL трафик
Управление на канала	Управлението на канала (QoS) следва да е налично и приложимо за всяко идентифицирано приложение
Управление на устройството	Всяко от устройствата в системата следва да се управлява посредством имплементация на REST based API за преглед на конфигурациите, изпълнение на команди и извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
Минимален брой интерфейси за управление	1 x 10/100/1000 out-of-band management port; 2 x 10/100/1000 интерфейси за отказоустойчивост; 1 x RJ-45 конзолен порт

Минимални изисквания за хард диск капацитет	120 GB (гигабайта) SSD хард диск
Логове и репорти	Всяко от устройствата в системата следва да разполага с минимум 120 GB (гигабайта) SSD хард диск за оптимална работа при съхранение на логовете и управление на рапортите. Всички механизми за мониторинг и генериране на рапорти следва да са налични локално за всяко от устройствата в системата без да е необходимо използване на допълнителни компоненти
Поддържани схеми за отказоустойчивост	Active-Passive конфигурации в Layer2/Layer 3. Active-Active конфигурации в Layer 2/Layer 3.; Механизъм за автоматично следене за прекъсване на работоспособността: интерфейс мониторинг, мониторинг на пътеката (path monitoring)
Форм фактор	Предназначена за вграждане в 19‘‘ шкаф и максимален размер 1U
Захранване (Средна / Максимална консумация на електроенергия)	250W (150/200 W/h)
Входно напрежение (Входяща честота)	100-240VAC (50-60Hz)

11.2. Система за защита на крайните точки

11.2.1. Минимални общи изисквания

Предложеното решение за защита на крайни точки трябва да може да:

- Предотвратява всички експлойти, включително тези, които използват неизвестни уязвимости на Zero-Day;
- Предотвратява всички злонамерени изпълними файлове, без да се изисква предварително познаване;
- Бъде ефективно в предотвратяването на експлойти и злонамерени програми без връзка или актуализации от сървърите за управление и / или ресурсите, базирани на облак.

Офертата да предлага решение за: усъвършенствана защита на крайни устройства (минимум 400 работни станции и 15 сървъра)

11.2.2. Минимални разширени функционални изисквания за защита на крайната точка

- Крайни клиенти

✓ Изпълнителят трябва да предложи решение за разширена защита на минимум 400 крайни точки и 15 сървъра.

✓ Предложеното решение да може да съществува съвместно или като самостоятелно решение с действащото решение за защита на потребителите (т.е. Anti-Virus)

- Управление

✓ Предложеното решение да се управлява от уеб-базиран графичен потребителски интерфейс (GUI).

✓ Предложеното решение трябва да има минимум тристепенна управленска структура, която се състои от конзола, управление и база данни. Решението да предлага възможност за инсталиране и на трите компонента в отделен хардуер или разпределени инсталации.

✓ Предложеното решение трябва да може да се инсталира на множество сървъри за управление на разпределени разположения и да се управлява от една уеб конзола.

✓ Предложеното решение да е в състояние да експортира своите логове във формат syslog към всяко решение за управление.

✓ Предложеното решение да е софтуерно базирано решение и да работи на операционна система Windows сървър.

✓ Предложеното решение трябва да може да се използва във виртуална среда (т.е. VMWare).

- Предотвратяване на експлоатацията

✓ Предложеното решение трябва да поддържа защитата на процесите и приложенията с възможност за добавяне към този списък на други приложения на трети страни и на собствени / персонализирани приложения.

✓ Предложеното решение да осигурява функция за конкретно извършване на мониторинг или изучаване на средата на ОРГАНИЗАЦИЯТА (т.е. инсталирани процеси и приложения в крайни точки).

✓ Предложеното решение трябва да е в състояние да предостави в реално време превенция срещу експлоатацията на уязвимости на приложението чрез блокиране на техники на експлоатация, които не се ограничават само до софтуерни логически недостатъци, корупция на паметта, отвличане на DLL и т.н.

✓ Предложеното решение трябва да е в състояние да предотврати неутрални или неразкрити експлоатации на всички уязвимости на приложението, като блокира техниките на експлоатация.

✓ Предложеното решение трябва да осигури възможност за извършване на мониторинг и предотвратяване на експлоатацията въз основа на редица техники на използване, без да се изисква връзка с Управленския сървър и / или Облачната услуга и без да се разчита на подписи.

✓ Предложеното решение трябва да предотвратява или блокира техниката на експлоатиране, да замрази процеса, да събере необходимата информация за анализ като името на процеса, пътя на файла, време на събитието, паметта, версията на операционната система, потребителския идентификатор, уязвимата версия на приложението и т.н. за този конкретен процес.

✓ Предложеното решение не трябва да използва интензивно ресурс от крайните точки (т.е. не повече от 1% CPU и не повече от 20MB – 50MB памет)

или хардуерно специфично използване на техниката за анализ като локален софтуер за виртуализиране на пясъчна кутия или виртуализиран контейнер.

✓ Предложеното решение трябва да актуализира модулите за техниката на експлоатация не повече от веднъж през Шест (6) месеца, за да се минимизират административните и оперативните разходи при изтегляне на актуализациите.

✓ Предложеното решение трябва да е в състояние едновременно да защитава всички приложения и процеси срещу техники на експлоатация.

- Предотвратяване на злонамерен софтуер

✓ Предложеното решение трябва да подкрепя защитата срещу изпълнението на злонамерени изпълними файлове.

✓ Предложеното решение да осигурява функция за конкретно извършване на мониторинг или изучаване на средата на ОРГАНИЗАЦИЯТА (т.е. инсталирани и изпълнявани процеси и приложения в крайните точки).

✓ Предложеното решение трябва да предостави възможност за контролиране на това, което може да бъде изпълнено по крайните точки на ОРГАНИЗАЦИЯТА (като например местоположението на папката, местоположението на мрежата, подвижните носители, неподписаните изпълними файлове и други).

✓ Предложеното решение трябва да предостави възможност за контрол и ограничаване на параметрите за това, как могат да се изпълняват изпълнимите файлове (без да се ограничават до местоположението на файловете за изпълнение, външни носители, местоположение на мрежата, възпроизвеждане на множество детски процеси, неподписани изпълними файлове и т.н.).

✓ Предложеното решение трябва да е в състояние да предотврати изпълнението на злонамерен софтуер, като използва злонамерени модули, за да насочи общите поведения на процесите, предизвикани от злонамерен софтуер .

✓ Предложеното решение не трябва да използва интензивно ресурс от крайните точки (т.е. не повече от 1% CPU и не повече от 20MB – 50MB памет) или хардуерно специфично използване на техниката за анализ като локален софтуер за виртуализиране на пясъчна кутия или виртуализиран контейнер.

- Неизвестен антивирусен анализ

✓ Предложеното решение трябва да има възможност да задава заявка за APT решение или разузнавателна информация за хеш стойности, за да провери дали е зловреден или доброкачествен.

✓ Предложеното решение трябва да има възможност да подаде потенциални злонамерени файлове в APT за Cloud през сървъра за управление на крайни точки.

✓ Предложеното решение трябва да има способността да разглежда доклада за анализ на злонамерен софтуер от сървъра за управление на крайни точки.

✓ Предложеното решение да не анализира файловете, които вече са били предоставени по-рано. Трябва да покаже, че файлът е идентичен и е подаден по-рано.

- Докладване.

Предложеното решение трябва да има следните навигационни табла за мониторинг на състоянието на сигурността и статуса на ОРГАНИЗАЦИЯТА:

- ✓ Табло за управление на сигурността на крайните точки;
- ✓ Табло за управление на събития за сигурността;
- ✓ Табло за управление на детайлите за заплахата;
- ✓ Данни за временния режим за таблото;
- ✓ Табло за управление на данните за грешки в сигурността;

- Предложеното решение да е в състояние да предостави уеб-базиран изглед на заплахите и злонамерения софтуер, както и да осигури експорт на регистрационни файлове за данни за заплахи или здравословно състояние в CSV формат.

11.3. Система за защита от изтичане на данни

Система за защита от изтичане на данни - (DLP) трябва да осигурява следното:

- Съхранение на най-различни събития и конфигурационна информация в сървърни системи за управление на база от данни - MS SQL;
- Управление от централизирана платформа, като дистанционно да бъдат управлявани и анализирани всички компоненти и събития свързани със защитата от изтичане на данни, към които са приложени най-различни видове полици и правила за осигуряване и ограничение на достъп и услуги;
- Информира в реално време за събитията свързани с нарушаването на полиците и правила осигуряващи сигурността на системата;
- Изготвя най-различни специфични доклади за компонентите на мрежата и текущото й състояние.

Системата за защита от изтичане на данни трябва да предоставя следните възможности:

- Предложената система трябва да използва Microsoft SQL Server за съхранение на DLP инциденти и конфигурация;
- Да притежава интегрирана web базирана конзола за менажиране на всички компоненти. Включващи конфигурационни политики, менажиране на инциденти и репорти, както и конфигурация на компонентите;
- Да включва Web Content Gateway компонент, който да осигурява висока производителност за SSL web proxy дешифриране;
- Два поддържа минимум следните два метода за идентификация:
  - ✓ RSA SecurID® authentication;
  - ✓ Certificate authentication.
- Системата трябва да поддържа интеграция на DLP с FCI (Microsoft File Classification Infrastructure);
- Системата трябва да осигурява функционалност за групово администриране въз основа на роли и политики;
- Системата трябва да се интегрира със следните продукти: Microsoft Active Directory, Microsoft Exchange 5.5/2000, Generic LDAP, Lotus Domino, Novell NDS, Sun/Netscape, LDAP, за да осигурява управление и отчитане на политиките налагани върху потребителите и групите;
- Решението за DLP трябва да предоставя библиотека от предварително дефинирани политики, които да покриват законодателството и регламентите в

областта на защитата на личните данни в световен мащаб и индустрията като PCI DSS;

- Системата трябва да предлага DLP метод за fingerprinting на структурирани данни, като например записи на клиенти. Също така политиките, използващи fingerprinting, трябва да се използват в корпоративната мрежа без задължителна VPN връзка;
- Предложеното решение за DLP да има възможност за откриване по съвпадение на частични текстове в документи и неструктурирани набори от данни, които са били fingerprinted;
- Системата трябва да позволява на администраторите да потвърждават точността на класификатора на fingerprint по време на създаването му;
- Предложеното решение за DLP трябва да поддържа машинното обучение;
- Предложеното DLP решение да осигурява интегрирано разпознаване на оптични символи и идентифициране на чувствителни данни, съхранявани в изображения;
- Системата да осигурява функция за идентифициране на ниско и бавно извличане на данни в случай, че потребителят е идентифициран да изпраща малки количества чувствителни данни (например данни от кредитни карти) за определен период от време;
- Предложеното DLP решение да предоставя набор от правила за "показател за риск от кражба на данни", предназначени да идентифицират кражбите на данни от злонамерени вътрешни лица и злонамерен софтуер;
- DLP решението да проверява файловите метаданни и да открива маркери за класифициране на документи;
- Предложеното DLP решение трябва да налага политики и технологии за откриване на съдържание във всички DLP канали (on-premises, endpoint and cloud data discovery);
- Решението трябва да поддържа минимум следните политики и технологии:

✓ Предварително дефинирани политики за съответствие и разкриване на IP адреси;

✓ Индикатора за риск от кражба на данни(анализ на поведението);

✓ Откриване по съвпадение на частични текстове в документи и неструктурирани набори от данни, които са били fingerprinted;

✓ Машинно обучение - откриване на защитено съдържание въз основа на обучение на системата DLP с набор от документи.

- Предложеното решение, трябва да предоставя възможност на служителите, администраторите и други групи хора, които управляват инциденти, да бъдат уведомени и чрез електронната си поща в реално време;
- Системата трябва да осигурява настройки за обширна защита на информацията и служителите, съобразена с политиките за защита на личните данни, въведени от държавите членки на ЕС;
- Решението да предотвратява загуба на данни, предоставени чрез прокси услуги за SSL/TLS декриптиране, които се използват за прилагането на

съответните за мрежовия трафик политики, отнасящи се към предотвратяването и загубата на данни;

- Предложеното решение за анализ на мрежовото съдържание да бъде софтуерно решение;
- Решението да предоставя възможност за анализ на мрежовото съдържание, както и възможност да използва категоризацията на уеб сайтовете създадена в политиките за предотвратяване загубата на данни с цел ограничаване или осигуряване на достъп до определени уеб сайтове;
- Решението за предотвратяване загубата на данни трябва да включва анализиращ механизъм за мрежовото съдържание, което да осигурява по-добра защитеност на системата и всеки един участник в нея;
- Системата трябва да предоставя и възможност за анализ и блокиране на трафика, използващ защитения HTTPS протокол. Gateway-а, отговарящ за мрежовото съдържание, да анализира информацията локално, без да изпраща информацията към други устройства - по този начин се поддържа целостта и защитеността на информацията. Използвайки политиките, отговарящи за забраняване или разрешаване на уеб сайтове, да може да се регулира и кои от сайтовете да бъдат наблюдавани и анализирани;
- Предложената система трябва да осигурява пълна DLP защита за крайните потребители, използващи Apple OS X, както при използването на следните приложения и функционалности:
  - ✓ Web HTTP/S (Safari, Firefox, Chrome);
  - ✓ И-мейл (поща, Outlook и Entourage);
  - ✓ При прехвърляне на информация върху сменяеми носители и оптични носители;
  - ✓ iCloud Drive и AirDrop;
  - ✓ Мониторинг на приложенията.
- Предложеното DLP решение да осигурява дълбока интеграция с браузърите Mozilla Firefox и Google Chrome на Windows и Apple OS X, за да позволи мониторинг на HTTP и HTTPS транзакции;
- Решението да предоставя подробна информация за инцидентите, генерирани за браузърите, да включва подробности за целевия уеб сайт и географското местоположение;
- Системата да следи и блокира прехвърлянето на файлове на мобилни устройства, като например таблети и смартфони с Android, използвайки протокола MTP (познат още като Windows Portable Devices);
- DLP решението за крайна точка трябва да поддържа мониторинг и блокиране на качвания на чувствителни данни в решения за съхранение в облак като DropBox, Google Диск, Microsoft OneDrive, Apple iCloud Drive и Box;
- DLP защитата за крайни клиенти трябва да осигурява функцията за байпас, която позволява DLP политиката да бъде деактивирана на управлявана крайна точка за определен период от време;
- Системата трябва да бъде предназначена да поддържа DLP функционалностите и на служители, които не са свързани с корпоративната мрежа;

- Решението да има възможност за проверка на мобилни устройства, които имат достъп до корпоративната мрежа, и да бъдат проверявани с помощта на правилата и политиките за DLP;
- Системата трябва да поддържа всички мобилни операционни системи, включително iOS, Android и Windows Mobile;
- Мобилният DLP агент да може да наблюдава и блокира данните, предавани в имейл съобщения, събития в календара и задачи;
- DLP решението за крайна точка трябва да поддържа проследяване на чувствителни данни, копирани на конкретно сменяемо медийно устройство;
- Предложеното решение за DLP да използва свой собствен MTA (mail transfer agent) за изпълнение на имейл DLP;
- Предложеното решение за DLP да поддържа правилата за електронната поща за Exchange Online;
- Решението трябва да осигурява и прилага политики за DLP на Microsoft Exchange Online, Office 365 и Microsoft Azure;
- DLP решението да разполага с функционалност за карантинни и-мейли, които нарушават фирмената политика за поверителни данни;
- Предложеното DLP решение трябва да предоставя контролен панел за Microsoft Outlook, който предоставя възможност за анализ на съдържанието на и-мейл преди те да достигнат до мрежата, като разглеждат детайлно частите от и-мейла - заглавия, тяло и прикачени файлове. Поддържани операционни системи: Windows и Apple OS X;
- Системата трябва да разполага с конзола за управление на данни, да предоставя както отчети, така и инцидентна информация. Отчетите за откриване имат функцията да показват сегменти от време за даден период;
- Предложената система трябва да предоставя възможност за планирани отчети - като позволява изготвянето на отчети и автоматично изпращане по и-мейл чрез PDF или CSV формат до конкретни заинтересовани страни;
- DLP решението да поддържа персонализиране на шаблони за отчети, използвайки филтри за отчети.

11.4. Система за откриване на потребителски идентификационни данни и разследване на сигнали за сигурност

- Открива компрометирани потребителски идентификационни данни: решението е необходимо бързо да открива хакери, които имат контрол върху идентификационните данни на мрежовия потребител, независимо от вектора на атаката или злонамерения софтуер;
- Открива компрометиране на привилегирован потребител: идентифицира конкретни атаки срещу привилегировани потребители, като DBA, които имат специален достъп до чувствителни системи;
- Да открива достъп до изпълнителни активи: възможност бързо да открива неоторизиран достъп до предварително дефинирани ресурси (например: съхранена важна информация), поради пробив от хакери или злонамерен софтуер.
- Да идентифицира поведението на служител / изпълнител, който извършва рисково или злонамерено поведение;

- Разследване на сигнали за сигурност: Да предоставя пълна информация за потребителите и активи, свързани с предупреждения за сигурност AV софтуер и DLP решения;
- Да създава проследяване на сесията на потребителя от съществуващите логове;
- Да анализира и сравнява сесии от всички потребители с цел откриване на не нормално поведение;
- Решението е необходимо да бъде оразмерено за 1000 потребителя и да няма лицензно ограничение на количеството лог информация, което трябва да бъде анализирано и събирано;
- Решението да се лицензира на брой потребители.
- Да събира логове от:

✓ Устройства за сигурност;
✓ Сървъри и крайни клиентски станции;
✓ Мрежови устройства;
✓ Бази Данни;
✓ Активност на приложението;
✓ Активност на потребители.

11.5. Система за управление на уязвимости

Функционални изисквания на система за управление на уязвимости:

- Да сканира системи с публични и частни IP адреси за актуални уязвимости в сигурността.
- Да има капацитет за сканиране на неограничен брой IP адреси, без ограничение на броя на сканиранията.
- Да не причинява смущения в работата на мрежата и устройството по време на сканирането.
- Да има възможност за управление на сканирането.
- Да идентифицира OS, инсталирания софтуер, активни услуги, състояние на портове, използвани протоколи, конфигурации, зловреден софтуер, експлойти.
- Да детайлизира информация за инсталирани сертификати.
- Да дава OS и софтуер.
- Да идентифицира и приоритизира рискове, произтичащи от откритите уязвимости, включително и Zero-Day.
- Да предоставя информация за идентификацията по CWE и оценката по CVSS на известните вече уязвимости, открити в системата.
- Да предлага решения за смекчаване на въздействието на риска и отстраняване на откритите уязвимости.
- Да изготвя подробни доклади за изброените по-горе изисквания, включително и за използваните проби и получените в резултат отговори.
- Да гарантира сигурността на данните при събиране, съхранение и пренасяне чрез криптиране и контрол на достъпа.
- Да има възможност за Brutefoce на пароли за широка гама от услуги, включително SMB/Windows/CIFS server, PostgreSQL database, IBM DB2 database, MySQL database, Microsoft SQL Server database, HTTP server (basic authentication),

HTTPS server (basic authentication), Secure Shell server, Telnet server, File Transfer Protocol server, BSD Remote Execution server, BSD Remote Login server, BSD Remote Shell server and Simple Network Management Protocol (SNMP).

- Да позволява на потребителите да създават и изпълняват кампании за извършване на социални инженерни атаки, включващи злонамерен уебсайт, фишинг по имейл и кампании за експлоатация на USB. Продукта трябва да проследява компрометираните цели и да представя проследяваните данни в социални доклади.
- Да има възможност за осигуряване на одити и експлоатации на уеб приложения, включително покритие на OWASP Top 10 злонамерености. Като например включване на отдалечени файлове, инжектиране на команди, скриптове между страници и SQL инжекции.
- Лицензът за ползване на софтуера следва да е безсрочен.

Минимални технически изисквания към елементите на системата за управление на уязвимости:

- Изисквания към хардуера:
- ✓ 2 GHz + процесор;
- ✓ Налична е 4 GB RAM;
- ✓ 1 GB свободно дисково пространство.
- операционната система:
- ✓ 64-битови версии на следните платформи се поддържат;
- ✓ Ubuntu Linux 14.04 LTS;
- ✓ Ubuntu Linux 16.04 LTS;
- ✓ Microsoft Windows Server 2008 R2;
- ✓ Microsoft Windows Server 2012 R2;
- ✓ Microsoft Windows 10;
- ✓ Microsoft Windows 8.1;
- ✓ Microsoft Windows 7 SP1 +;
- ✓ Red Hat Enterprise Linux Server 7.1 или по-нова версия;
- ✓ Red Hat Enterprise Linux Server 6.5 или по-нова версия;
- ✓ Red Hat Enterprise Linux Server 5.10 или по-нова версия
- Изисквания към БРАУЗЪРИ:
- ✓ Google Chrome;
- ✓ Mozilla Firefox;
- ✓ Microsoft Internet Explorer 11.

12. Изисквания към усъвършенстване на система за защита на личните данни

12.1. Общи положения

При извършването на дейностите следва да:

- бъдат съблюдавани изискванията и предписанията на общия регламент относно защитата на личните данни на физическите лица и националното законодателство;
- бъде установено текущото състояние на централата по отношение на съхраняването и обработването на личните данни;

- бъдат направени препоръки при наличие на несъответствие с изискванията на регламента;
- се дадат предложения за решения, адресиращи разликите (GAPs) между текущото състояние и изискванията на регламента (GDPR);
- се проведе обучение на служителите на възложителя, отговорни за събиране, обработване и съхранение на лични данни.

12.2. Обхват на анализа на несъответствията (GAP анализ)

12.2.1. Организационно-управленска фаза

- Преглед, цялостен анализ и оценка на текущите регистри и регистрацията на възложителя в Комисия за защита на личните данни („КЗЛД“);

Анализът следва да е фокусиран върху съответствието на вътрешните фирмени актове, регистри и процедури с изискванията на сега действащия закон в Република България и новия Регламент 2016/679.

- Преглед, подробен анализ и оценка на всички вътрешни документи, регулиращи процесите по обработване, съхранение и трансфериране на лични данни - вътрешни правила, декларации, заповеди, процедури, договори, бизнес кореспонденция и други;
- Изготвяне / осъвременяване и първоначално съгласуване на Инструкция (вътрешни правила) за защита на личните данни;
- Изготвяне и първоначално съгласуване на съпътстващи Инструкцията процедури и документи, в това число:

✓ Процедура за събиране, обработване и защита на личните данни, предоставяни от кандидати за работа и от служители (онлайн и на хартиен носител);

✓ Декларации за съгласие за предоставяне, обработване и трансфер на лични данни, които се подписват от служители, контрагенти, клиенти и други, при събиране и предоставяне на информация под формата на лични данни;

✓ Процедура за оценка на въздействието на съхраняваните лични данни и изготвяне на протоколи и въпросници за извършване на законосъобразна оценка на въздействието;

✓ Процедура за унищожаване на личните данни, съобразно разпоредбите на приложимото Българско законодателство и на Инструкцията за защита на личните данни на възложителя и изготвяне на протоколи за унищожаване на лични данни в тази връзка;

✓ Изготвяне на списък с процедури и правила, които следва да бъдат периодично допълвани и изменяни.

12.2.2. Организационно-техническа фаза:

- Информационни потоци:

✓ Определяне на входни и изходни вектори, по които информацията влиза и напуска организацията;

✓ Проверка, каква част от данните представляват сами по себе си или в съвкупност лични данни, които попадат под изискванията на регламента;

✓ Препоръки за защита и оптимизация.

- Местоположение на лични данни:

✓ Идентифициране на системите в организацията, които съдържат или могат да съдържат на свои носители лични данни;

✓ Определяне на използвани бази от данни. Дефиниране на лични данни или съвкупност от данни, които могат да бъдат окачествени като лични;

✓ Изготвяне на препоръки за:

- Защита срещу посегателство отвън;
- Защита срещу изтичане навън;
- Защита срещу посегателства отвътре;
- Криптиране;
- Анонимизация на лични данни;
- Псевдонимизация на лични данни.

- Вътрешен обмен на лични данни:

✓ Определяне на системите и каналите, по които се обменят лични данни;

✓ Определяне на процеси и процедури за одобрение, потоци на движение на данните;

✓ Изготвяне на препоръки за защита на обмена на данни между системите и приложенията;

✓ Оптимизиране на йерархията за контрол и одобрение.

- Права за достъп:

✓ Преглед на групите потребители, ролите за достъп до системите и приложенията, идентифициране на тези, които работят с лични данни;

✓ Преглед на начините за раздаване на права на служителите в следните случаи:

- Постъпване на работа;
- Напускане на работа;
- Преместване в структурата на организацията.

✓ Повишена защита на системите чрез разделяне на нивата на достъп и ограничаването им до минимума необходими за изпълнение на служебните задължения;

✓ Препоръки за защита и оптимизация на ролите и правата за достъп до информацията в организацията.

- Постоянно наблюдение:

✓ Проверка на средствата за документиране и наблюдение на достъпа до лични данни;

✓ Оценка на съхранението на системната мета-информация, срокове и начин на защита;

✓ Степени на съхранение на предишното състояние на данните;

✓ Изготвяне на препоръки за подобрение.

- Превенция на инциденти

✓ Оценка на възможните пропуски в сигурността при обработка на данните;

✓ Оптимизиране на работния процес, позволяващо превантивно да се идентифицират и решават потенциалните проблеми;

✓ Минимизиране на риска, чрез повишаване сигурността на цялата комуникационна инфраструктура и намаляване на възможността за сривове и пробиви;

✓ Изготвяне на предложение за комплексно техническо решение, което в максимална степен да удовлетвори реализацията на защитената работа в организацията. Предложението да отговаря на съвременните добри световни практики.

- Реакция след настъпване на инцидент:

✓ Препоръки за повишаване ефективността при кризисни мерки (възстановяване от сривове, информационни загуби и други бедствия);

✓ Оценка на щетите и загубите. Ограничаване на периметъра;

✓ Процедура за докладване на проблема до отговорните институции.

12.3. Изготвяне на доклад

- На базата на събраната информация и направените анализи и заключения по всички точки от 12.2, следва да бъде изготвен и предоставен Доклад за изпълнения Анализ на несъответствията;
- Докладът трябва да отрази текущото организационно-техническо състояние на дружеството, идентифицираните различия, необходими действия и препоръки за решения за привеждане в съответствие с изискванията на общия регламент;
- Докладът следва да бъде структуриран в съотвествие с двете направления на извършените дейности, а именно в две обособени части - Организационно-управленска и Информационно-техническа.

12.4. Обучение и подготовка на отговорните служители

Подготовка и провеждане на обучение на служителите, отговорни за събиране, обработване и съхранение на лични данни.

Обучението следва да обхване следните теми:

- „Какво са лични данни“?
- Проверка от КЗЛД - правомощия на органа, необходими документи;
- Инструкция на възложителя;
- Трансфер на лични данни;
- Новият регламент (GDPR) - в сила от 25.05.2018 година;
- Запознаване на служителите със съвременните заплахи в информационната сигурност;
- Правила при електронна обработка на лични данни;
- Изготвяне на програма за повишаване на квалификацията на служителите за справяне със заплахи в информационната среда.

V. Изисквания за осигуряване на безопасни условия на работа

При извършване на отделните видове работа трябва да се спазват изискванията на „Правилника за безопасност на труда при строително-монтажни работи” и „Правилника за безопасност на труда при експлоатирането на електрически уредби и съоръжения”.

Всички инсталатори и софтуеристи да се инструктират по техниката на безопасност и да им се направи инструктаж за безопасна работа непосредствено на работното място.

Преди започване на работа, инсталаторите да се снабдят с лични предпазни средства, съобразени с наличните на обекта предупредителни и указателни табели.

Работите за изпълнение на поръчката да започнат с писмено нареждане на наблюдаващото от страна на Възложителя лице.

Всички съоръжения да са заземени. Забранява се работата с неизправни инструменти, както и дейности, които противоречат на изискванията за охрана и безопасност на труда.

Обслужването на електрооборудването да се извършва само след изключване на устройството от електрическата мрежа.

Забранява се извършването на огневи работи и на други дейности, свързани с отделянето на топлина в близост до устройствата на пожарогасителните инсталации.

Възложител
Изп. директор: .....п.....
инж. Ж. Динчев

Изпълнител
Представляващ: .....п.....
П. Петров

„ТЕЦ МАРИЦА ИЗТОК 2“ ЕАД
6265 Ковачево, обл. Стара Загора, тел. 042/662 214, 042/662 014
факс: 042/662 000, 042/662 507, e-mail: tec2@tpp2.com

Management System ISO 9001:2008 ISO 14001:2004 OHSAS 18001:2007 TÜVRheinland CERTIFIED www.tuv.com ID 9105038729

с. КОВАЧЕВО "ТЕЦ МАРИЦА ИЗТОК 2"ЕАД обл. СТАРА ЗАГОРА

РЕПУБЛИКА БЪЛГАРИЯ ДЪРЖАВНА АГЕНЦИЯ "НАЦИОНАЛНА СИГУРНОСТ" Вх.№ СЗ-32-1547 Екз.№ 1 от 23.04.2018

УТВЪРДИЛ: .....

инж. ЖИВКО ДИНЧЕВ,
РЪКОВОДИТЕЛ НА ОЕ

23. 04. 2018

СХЕМА ЗА КЛАСИФИКАЦИЯ НА ЕТАПИТЕ ЗА СКЛЮЧВАНЕ И ИЗПЪЛНЕНИЕ НА ДОГОВОР

чрез процедура на договаряне с публикуване на обявление за сключване на договор с обмен на класифицирана информация

I. ПРЕДМЕТ НА ДОГОВОРА: „Изграждане на център за киберсигурност за нуждите на „ТЕЦ Марица изток 2“ ЕАД. Усъвършенстване на съществуващата система за личните данни и създаване на надеждна киберзащита за нея в изпълнение на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г.“

При изпълнение на договора ще възникне необходимост от обмен на класифицирана информация. За реализиране на това свое задължение определени лица от изпълнителите трябва да се запознаят и ползват:

- Дългосрочна ПРОГРАМА (за срок от четири години) за осигуряване киберзащитата на „ТЕЦ Марица изток 2“ ЕАД;
- Краткосрочен ПЛАН (за срок от две години) за осигуряване киберзащитата на „ТЕЦ Марица изток 2“ ЕАД

с ниво на класификация „Поверително“, класифицирани на основание т. 3 от Раздел III на Приложение № 1 към чл. 25 от ЗЗКИ.

Предвижда се предоставяне, обработване или съхраняване на класифицирана информация при изпълнителите. Предвижда се създаване на класифицирана информация от изпълнителите в хода на изпълнение на договора. За целта е необходимо изпълнителите да имат издадени удостоверения за сигурност с право да обработват и съхраняват класифицирана информация в своите помещения и сертифицирана регистратура за национална класифицирана информация най-малко до ниво „Поверително“. Ако изпълнителите не притежават сертифицирана АИС/М, цялата класифицирана информация ще се създава в РКИ на възложителя.

II. СХЕМА ЗА КЛАСИФИКАЦИЯ - по чл. 4 от „Наредба за общите изисквания за гарантиране на индустриалната сигурност“, включваща следните етапи:

№ по ред	Етапи на изпълнение на поръчката	Срок	Дейности	Задачи	Ниво на класификация на етапите
1.	Подготвителни действия по стартиране на процедурата за възлагане на обществена поръчка	15.03.2018 г.	Изготвяне мотивирано становище от служителя по сигурността на информацията за определяне нивото на класификация на обществената поръчка.	Определяне нивото на класификация на етапите, вида на процедурата, срока и реда за изпълнение на поръчката.	Не класифицирано
1.1.	Изготвяне от възложителя на дългосрочна ПРОГРАМА (за срок от четири години) за осигуряване киберзащитата на дружеството.	12.03.2018 г.	Определяне на дъглосрочната вътрешноведомствена, административно - организационна политика на дружеството за киберсигурност с прилагане на съвременни технологични решения за регламентирано и контролирано оптимално използване на съществува - щата IT - инфраструктура в централата.	Съгласно указания на ДАНС рег. № RB202002-001-04/И-3-1085 от 24.07.2017 г. и рег. № И-1724 от 20.09.2017 г.	„Поверително“
1.2.	Изготвяне от възложителя на краткосрочен ПЛАН (за срок от две години) за осигуряване киберзащитата на дружеството.	12.03.2018 г.	Определяне на приоритетите в краткосрочен план за реализиране на нова Производствена, Административна и Публична компютърна мрежа.	Съгласно указания на ДАНС рег. № RB202002-001-04/И-3-1085 от 24.07.2017 г. и рег. № И-1724 от 20.09.2017 г.	„Поверително“
1.3.	Изготвяне на схема за класификация на етапите и съгласуване с ДАНС.	15.03.2018 г.	Определяне предмета на договора, етапите на изпълнение на поръчката, включително тези, за които е необходим достъп до КИ, дейностите и задачите във връзка със сключването и изпълнението му.	Съгласуване с компетентните органи по чл. 95, ал. 3 от ЗЗКИ	Не класифицирано
1.4.	Изготвяне на докладна записка за стартиране на обществената поръчка.	27.04.2018 г.	Посочване на изисквания за изпълнение на поръчката и за осигуряване на условия за защита на класифицирана информация.	Определяне критериите за предварителен подбор на участниците, включително наличие на удостоверения за сигурност.	Не класифицирано
1.5.	Обявяване на ОП	Съгласно ЗОП	Обявяване на ОП в Регистъра на АОП и в профила на купувача в интернет сайта на централата. Подготвяне и подаване на заявления за подбор и оферти от кандидатите в ОП.	Подготовка на документа - ция в съответствие с изискванията на ЗОП и НОИГИС. Включване в проекта на договора изискванията на раздел II от НОИГИС.	Не класифицирано

1.6.	Разглеждане на подадените заявления	Съгласно ЗОП	Провеждане на процедурата. Определяне на кандидатите, отговарящи на критериите за подбор. Изготвяне на протокол от комисията за подбор на кандидатите, които ще бъдат поканени за представяне на оферта и провеждане на преговори.	Определяне на комисия за излъчване на изпълнители. Членовете на комисията да отговарят на изискванията на ЗОП. Проверка за съответствие на заявленията с изисква - нията на възложителя. Потвърждаване от компетентния орган по чл. 95 ал. 3 от ЗЗКИ на наличието и валидността на издадени удостоверения за сигурност, разрешения за достъп или потвърждения на кандидатите. Отстраняване на кандидати, неотговарящи на критериите за подбор и изискванията за осигуряване на условия за защита на класифицирана информация. Не се предвижда предос - тавяне на класифицирана информация.	Не класифицирано
1.7.	Разглеждане на подадени оферти, оценка и договаряне.	Съгласно ЗОП	Отправяне на покани за представяне на оферти от допуснатите кандидати. Разглеждане на първоначални оферти. Провеждане на договаряне.	Определяне на изпълнител. Задължително посочване на лице, определено за ССИ от страна на изпълнителя. Не се предвижда предос - тавяне на класифицирана информация.	Не класифицирано
2.	Сключване на договор.	Съгл. ЗОП и устава на ТД	Подготвяне и подписване на договор с изпълнителя, спечелил ОП.	Подготвяне договора и включване на клаузи, касаещи специфичните изисквания за защита на класифицирана информация по чл. 10 от НОИГИС. Определяне на лице от Възложителя по чл. 105 от ЗЗКИ и лице от Изпълнителя съгласно чл. 12 от НОИГИС за контрол и спазване на разпоредбите по ЗЗКИ.	Не класифицирано

3.	Изпълнение на договора.	Съгласно ЗОП	Определяне на кръга от лица на изпълнителя за запознаване с дългосрочната ПРОГРАМА и краткосрочния ПЛАН за осигуряване на киберзащитата на „ТЕЦ Марица изток 2“ ЕАД. Провеждане на обучение на определените лица в областта на ЗЗКИ. Запознаване на определените лица с програмата и плана. Предоставяне на класифици - рана информация за обработ - ване при изпълнителите. Включва реално осъществя - ване от изпълнителя на дейностите по договора и е свързан с достъп или необходимост от работа с класифицирана информация.	Контрол при изготвяне от изпълнителя на проектна и работна документация. При необходимост от класифициране на тази информация и ако изпълнителя не притежава сертифицирана АИС/М, същата ще се създава в РКИ на възложителя. Постоянен контрол за спазване на изискванията за изпълнение на договора, ЗЗКИ и актовете по неговото прилагане от задължените субекти.	„Поверително“
4.	Действия след приключване на договора.	Съгласно чл. 13 и чл. 17 на НОИГИС и изискванията на ЗЗКИ	Връщане от изпълнителя на цялата документация или материали, съдържащи класифицирана информация, получени от възложителя или създадени в хода на изпълнението на договора.	Осигуряване на мерки за недопускане на нерегламентиран достъп до класифицирана информация, узната при изпълнение на договора.	„Поверително“

Изготвил,

.....

инж. КОНСТАНТИН КОЛЕВ

Служител по сигурността на информацията

СЪГЛАСУВАНО:

Директор УСП КИ

.....

Виолета Кръстева

.....

ДЪРЖАВНА АГЕНЦИЯ „НАЦИОНАЛНА СИГУРНОСТ“

ДЪРЖАВНА АГЕНЦИЯ „НАЦИОНАЛНА СИГУРНОСТ“ РЕПУБЛИКА БЪЛГАРИЯ