IT CONSULTING COMPANY

София 1233
Бул. Сливница 141-143, етаж. 2
тел. +359 (2) 980 91 79

www.chorus.bg

ДО: **Софийска вода АД**

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

по обява **47410/ZB-3406**

за обществена поръчка на стойност по чл. 20, ал. 3 от ЗОП

Кратко описание на предложението:

В съответствие с минималните технически изисквяния по обява **47410/ZB-3406**, Корус ООД предлага да внедри и поддържа за период от една година 900 броя от продуктовия пакет **Trend Micro Smart Protection Complete**, който напълно покрива заложените технически изисквания (детайлно описание на съответствията може да се открие в **Приложение 1**).

В допълнение на доставката на лицензи за посочените продукти, Корус ООД ще извърши първоначално внедряване на продуктите (съобразено с конкретните изисквания, предоставени от страна на Софийска вода АД), както и пълна поддръжка от второ ниво на продуктите за периода на лицензa.

Поддръжката, съобразена със заложените технически изисквания ще отговаря на следните минимални нива на услуга:

- Период: 9x5x365 (девет часа, пет дни в седмицата (от понеделник до петък), съобразено с работното време на „Софийска вода" АД – 08:00 – 19:00)
- Време за реакция – до 4 (четири) часа след подаване на сигнал от страна на Възложителя;
- Време за отстраняване на проблеми, свързани с конфигурация и/или настройка на системата – до 3 работни дни след приемане на сигнал
- Време за отстраняване на проблем, който касае намесата на Производителя - до 1 (един) месец след приемане на сигнал;
- Ескалация на инциденти към производителя, при необходимост;
- Ескалация към производителя при проблеми с продуктите, при необходимост;
- Поддръжката да се извършва на български език;
- Получаване и внедряване на нови продуктови обновявания за срока на договора;
- Обновяване на продуктовите дефиниции за срока на договора;
- Поддръжка по електронна поща, Web портал или по телефона.
- 24 x 7 (24 часа в денонощието, 7 дни в седмицата) телефонна поддръжка;
- Приоритетен достъп до Support.

TREND MICRO Gold Partner

IT CONSULTING COMPANY

София 1233
Бул. Сливница 141-143, етаж. 2
тел. +359 (2) 980 91 79

www.chorus.bg

ДО: **Софийска вода АД**

ПРИЛОЖЕНИЕ 1

към ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ по обява 47410/ZB-3406

за обществена поръчка на стойност по чл. 20, ал. 3 от ЗОП

2.1. Защита и централизирано управление на потребителски устройства:	
○ **Защита за Windows базирани крайни точки** - работни станции, преносими компютри, таблети, виртуални крайни точки (VDI - платформи).	OfficeScan + VDI plugin
▪ Защита срещу зловреден код: вируси, троянски коне, червеи, рансъмуер, шпионски софтуер и друг зловреден код	OfficeScan
▪ Блокиране на достъпа до зловредни уеб сайтове посредством уеб репутация;	OfficeScan
▪ Контролиране на мрежовата активност посредством защитна стена (Firewall);	OfficeScan (firewall)
▪ Криптиране на твърдите дискове, с централизирано управление на ключовете;	Endpoint Encryption (Full disk encryption)
▪ Криптиране на файлове и директории;	Endpoint Encryption (File & Folder encryption)
▪ Защита срещу уязвимости, включително срещу експлойти, за които все още няма обновявания (пачове) от съответния производител;	Intrusion Defense Firewall (virtual patching)
▪ Криптирана централизирана карантина;	OfficeScan
▪ Самозащита на софтуера за защита срещу изключване, промяна или модификация от страна на потребителя или злонамерен софтуер;	OfficeScan

TREND MICRO Gold Partner

▪ Контрол на разрешените приложения посредством „Бял списък / Черен списък“ (whitelist/blacklist), изготвен чрез прилагане на едно или повече правила, дефинирани с помощта на следните критерии: категория на приложението, репутация, производител, сертификат на производителя и други;	Endpoint Application Control
▪ Интегрирана, уеб базирана конзола за управление и наблюдение;	Control Manager
▪ Наличие на услуга за предотвратяване на епидемии;	OfficeScan (Outbreak Prevention Services)
▪ Интеграция с Active Directory;	OfficeScan
▪ DLP защита за крайните клиенти, с възможност за криптиране на чувствителни файлове при копиране върху незащитен носител;	OfficeScan DLP plug-in / Endpoint Encryption
▪ Централизирано управление, наблюдение, създаване на политики и отчетност (reporting);	Control Manager
▪ Възможност за отдалечена (централизирана) инсталация и деинсталация;	OfficeScan
▪ Интегрирана, уеб базирана конзола за управление и наблюдение.	OfficeScan / Control Manager
○ **Защита на Mac базирани компютри**	
▪ Защита срещу зловреден код: вируси, троянски коне, червеи, рансъмуер, шпионски софтуер и друг зловреден код;	Security for MAC
▪ Блокиране на достъпа до зловредни уеб сайтове посредством уеб репутация;	Security for MAC
▪ Контролиране на мрежовата активност посредством защитна стена (Firewall);	-
▪ DLP защита на чувствителна информация.	-
○ **Защита и управление за мобилни устройства:**	
▪ Защита и централизирано управление на Android и iOS мобилни устройства и таблети срещу заплахи и зловреден и шпионски софтуер;	Mobile Security

▪ Централизирано провизиране на WiFi-мрежи;	Mobile Security
▪ Интегрирана, уеб базирана конзола за управление и наблюдение и отчетност;	Mobile Security / Control Manager
▪ Интегрирана, уеб базирана конзола за управление и наблюдение.	Mobile Security / Control Manager
2.2. Защита и централизирано управление за сървърна инфраструктура	
○ **Защита и централизирано управление на шлюза за електронна поща (Mail Gateway Protection)**	
▪ Защита и централизирано управление на шлюза за електронна поща от спам, фишинг, нежелана поща, зловреден софтуер, зловредни URL препратки или други атаки;	InterScan Messaging Security
▪ Централизирано управление – използване и модифициране на предварително създадени или създаване на нови филтри и политики;	InterScan Messaging Security
▪ Дублиране и мащабируемост на услугата;	InterScan Messaging Security / Cluster
▪ Централизирана карантина; управление на карантината за блокирани електронни писма;	InterScan Messaging Security
▪ Защита на изходящия пощенския трафик с DLP;	InterScan Messaging Security iDLP plugin
▪ Интеграция с Microsoft Active Directory;	InterScan Messaging Security
▪ Интегрирана, уеб базирана конзола за управление и наблюдение.	InterScan Messaging Security / Control Manager
○ **Защита и централизирано управление за корпоративен пощенски сървър – Microsoft Exchange Server**	
▪ Защита и централизирано управление от спам и фишинг, нежелана поща, технологии за блокиране на писма съдържащи зловредни URL адреси, зловреден софтуер, и други уеб заплахи;	ScanMail Suite for Microsoft Exchange
▪ Защита на чувствителна информация с DLP	ScanMail iDLP plugin

▪ Централизирана карантина на блокирани електронни писма	ScanMail Suite for Microsoft Exchange
▪ Интеграция с Microsoft Active Directory;	ScanMail Suite for Microsoft Exchange
▪ Интегрирана, уеб базирана конзола за управление и наблюдение.	ScanMail Suite / Control Manager
○ **Защита и централизирано управление за Интернет шлюз (Internet Gateway Protection)**	
▪ Антивирусна и анти-шпионска защита, технология за репутацията на уеб страниците;	InterScan Web Security
▪ Автоматично разпознаване и контрол на приложения, вкл. уеб базирани;	InterScan Web Security
▪ Политики за достъп, базирани на категории уеб сайтове, специфични приложения или отделни уеб сайтове / уеб страници; възможност за ограничаване на достъпа само от определени потребители или работни станции; ограничаване на достъп за конкретно указан период от време и други;	InterScan Web Security
▪ Възможност за осигуряване на отказоустойчивост или по-голям капацитет на Интернет шлюза, посредством виртуални устройства за филтрация;	InterScan Web Security / Cluster
▪ Възможност политиките за уеб трафика да се прилагат и върху потребители, работещи извън мрежовата инфраструктура на компанията;	InterScan Web Security **as a Service**
▪ Интеграция с Microsoft Active Directory;	InterScan Web Security
▪ Защита срещу изтичане на информация с DLP;	InterScan Web Security iDLP plugin
▪ Интегрирана, уеб базирана конзола за управление и наблюдение.	InterScan Web Security / Control Manager
○ **Защита и централизирано управление за SharePoint сървъри**	
▪ Интегрирана защита срещу злонамерен софтуер, злонамерени връзки в съдържанието на SharePoint;	PortalProtect for Microsoft SharePoint

▪ Интеграция с Microsoft Active Directory;	PortalProtect for Microsoft SharePoint
▪ Защита на съдържанието с DLP;	PortalProtect for Microsoft SharePoint iDLP plugin
▪ Интегрирана, уеб базирана конзола за управление и наблюдение.	PortalProtect for Microsoft SharePoint
○ **Защита и централизирано управление за Windows и Linux файлови сървъри**	
▪ Защита в реално време срещу компютърни вируси/шпионски софтуер, троянски коне, червеи и други рискове за Windows и Linux базирани файлови сървъри;	OfficeScan / Server Protect for Windows/Linux
▪ Възможност за създаване на различни графици за сканиране;	OfficeScan / Server Protect for Windows/Linux
▪ Възможност за различни действия при сканиране;	OfficeScan / Server Protect for Windows/Linux
▪ Наличие на услуга за предотвратяване на епидемии;	OfficeScan / Server Protect for Windows/Linux (Outbreak Prevention Services)
▪ Възможност за централизирано инсталиране и управление на сканиранията;	OfficeScan / Server Protect for Windows/Linux
▪ Възможност за криптиране на файлове и папки, както и DLP защита (за Windows);	File&Folder Encryption; OfficeScan iDLP plugin
▪ Контрол на приложенията – възможност за налагане на „Бял списък“ (Whitelist) както за конкретни приложения, така и за категории / производители;	Application Control
▪ Централизирано управление с интеграция с Active Directory;	Control Manager
▪ Самозащита на софтуера срещу изключване, промяна или модификация от страна на потребителя или злонамерен софтуер.	OfficeScan
○ **Защита за Skype for Business Server 2015**	
▪ Защита в реално време от злонамерени приложения – компютърни	IM Security for Microsoft

TREND MICRO Gold Partner

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

вируси, шпионски софтуер, троянски софтуер, компютърни червеи и други рискове за сигурността;	Lync Server
▪ Защита от разпространение на файлове с нецензурно или недопустимо по други причини съдържание;	IM Security for Microsoft Lync Server
▪ Защита от злонамерени уеб връзки, включително във файлове, изпращани посредством незабавни съобщения. Репутация на връзките;	IM Security for Microsoft Lync Server
▪ DLP защита на изпращаните незабавни съобщения и файлове;	IM Security for Microsoft Lync Server iDLP plugin
▪ Интегрирана, уеб базирана конзола за управление и наблюдение.	Control Manager
2.3. Защита за облачна инфраструктура (Google Drive)	
○ Интеграция със споделянето на файлове в Google Drive;	Cloud App Security
○ Защита срещу зловреден код;	Cloud App Security
○ Защита срещу изтичане на информация посредством DLP;	Cloud App Security DLP
○ Интеграция с Active Directory;	Cloud App Security / Google Apps AD Sync
○ Централизирано управление, наблюдение и отчетност.	Control Manager
2.4. Централизирано управление, наблюдение и отчетност за цялата инфраструктура	
○ Централизирано управление на всички предложени продукти посредством уеб конзола. Централизирано наблюдение на продуктите, изготвяне на отчети, базирани на цялата събрана информация от конзолата;	Control Manager
○ Прилагане на централизирани политики върху всички съставни продукти от решението;	Control Manager
○ Възможност за управление на продуктите като група (в зависимост от тяхната функция, ако са инсталирани повече от един или на повече от едно място);	Control Manager
○ Интеграция с Active Directory;	Control Manager

○ Възможност за автоматични уведомления на администраторите по електронна поща за инциденти свързани с:	Control Manager
▪ Активност на зловреден код;	Control Manager
▪ Инциденти свързани с DLP;	Control Manager
▪ Атаки на мрежови уязвимости;	Control Manager
▪ Обновявания на продуктите.	Control Manager
○ Възможност за интегриране със съществуващата Система за Информационна Сигурност и Управление на Събития (Security Information & Event Management, SIEM) на McAfee.	OfficeScan / Control Manager

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

IT CONSULTING COMPANY

София 1233
Бул. Сливница 141-143, етаж. 2
тел. +359 (2) 980 91 79

www.chorus.bg

ДО: **Софийска вода АД**

ПРИЛОЖЕНИЕ 3 –
„КРАТКО ОПИСАНИЕ НА ПРОДУКТИТЕ“

към **ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ** по обява **47410/ZB-3406**
за обществена поръчка на стойност по чл. 20, ал. 3 от ЗОП

Trend Micro Smart Protection Complete

Trend Micro Smart Protection Complete е цялостно решение за защита на мрежата и данните, което включва защита от зловреден софтуер, вируси, спам, решение за защита от изтичане на информация, решение за криптиране, контрол над приложенията, защита за портали и комуникационен сървър Lync.

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

Функционално описание (групиране) на продуктите, включени в пакета:

	Smart Protection Complete
TOOLS TO SIMPLIFY ONGOING MANAGEMENT AND SUPPORT OF THE SOLUTION	
Central Management	✓
On-premises, cloud, or Hybrid Deployment	✓
24x7 Support	✓
Integrated Data Loss Prevention	✓
ENDPOINT	
XGen™ Anti-malware	✓
Vulnerability Protection	✓
Virtual Desktop Integration	✓
Mac and Windows Security	✓
Server Security	✓
Endpoint Application Control	✓
Endpoint Encryption	✓
Mobile Security and Management	✓
Advanced Detection and Response	✓
EMAIL AND COLLABORATION	
Messaging Gateway	✓
Mail Server Security for Microsoft Exchange	✓
Mail Server Security for IBM Domino	✓
Instant Messaging Security for Microsoft Lync	✓
Microsoft SharePoint Security	✓
Security for Microsoft Office 365, Box, Dropbox	✓
WEB	
Secure Web Gateway	✓

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

Кратко описание на модулите:

1. **Gateway protection**

Спира имейл и уеб заплахи, преди да влязат в организацията

InterScan Messaging Security

Осигурява защита на шлюза за електронна поща срещу зловреден софтуер,спам, фишинг, нежелана поща, зловредни URL препратки или други зловредни атаки.

InterScan Web Security

Осигурява защита на уеб шлюза чрез уеб репутация в реално време, филтриране на URL линкове, блокиране на зловредни сайтове. Предоставя сигурен достъп до актуалните уеб приложения и социални медии.

2. **Mail server protection**

Блокира спам, зловредни URL и малуеър, достигнали до пощенските кутии върху мейл сървъра.

ScanMail Suite for Microsoft Exchange

Осигурява защита на пощенския сървър (Microsoft Exchange Server) срещу вируси, спам, фишинг, писма съдържащи зловредни URL адреси и други таргетирани атаки.

3. **Защита на файлови сървъри**

Защита на сървърите от малуеър и други уеб заплахи

OfficeScan

Осигугурява защита на Windows сървъра като част от цялостната защита на крайните точки, като консолидира крайните устройства в една унифицирана инфраструктура.

ServerProtect for Microsoft Windows/Novell NetWare

Защитава Windows и Novell NetWare файлови сървъри срещу уеб заплахи, шпионски вирvси и други зловредни софтуери.

ServerProtect for Linux

Защитава Linux файлов сървър срещу компютърни и шпионски вируси, зловреден софтуер и други рискове в реално време, като предоставя възможност за автоматизирано обезвреждане на заплахата и възстановяване на системата.

4. Защита на клиентски работни места / мобилни устройства

Защита на всяка крайна точка – с най-надеждните технически средства

OfficeScan

Осигурява цялостна защита на крайните точки (работни станции, преносими компютри, таблети, виртуални крайни точки (VDI-платформи) срещу троянски кон, червеи, шпионски софтуер и други зловредни кодове.

Intrusion Defense Firewall

Използвайки вграден модул в *OfficeScan*, осигурява хост базирана защита на мрежово ниво срещу непознати заплахи на операционната система и клиентските приложения.

Mobile Security (Suite Edition)

Осигурява централизирано управление и защита на мобилни устройсва (Android, iOS) срещу заплахи и зловреден софтуер. Предоставя възможност за криптиране и отдалечено изтриване на информацията на устройствата.

Security for Mac

Осигурява комплексна защита за MAC устройства чрез внедряване на политики за сигурност на всички крайни точки.

5. Централизирано управление

Улеснява администрацията чрез централизиране на политиките по защита в единна, уеб базиран конзола.

Control Manager

Централизирана конзола за управление, събиране на логове и отчети, обхващаща всички решения, за предоставяне на пълна информация и контрол върху защитата на отделните потребители.

6. Интегрирано DLP решение за крайните устройства

Централизирано прилагане на политики срещу умишлена или случайна загуба на чувствителна информация.

- Възможност за контрол на устройствата, включително задаване на специфични правила за отделни устройства (напр. чрез базиране по сериен номер.)
- Възможност за ограничаване или забраняване на употребата на преносими устройства (USB, CD/DVD и др.)
- Реагиране при неподходящо употребление на данни чрез ключови думи, регулярни изрази, бланки и др.
- Предупреждаване на служителите относно политиките за използване на корпоративни данни чрез сигнали, блокиране и искане за съгласие.
- Осигуряване съответствие с нормативни уредби чрез употреба на външни шаблони
- Намалява времето за одит, налагане на правила и дейности по разследване на инциденти.
- Лесно внедряване и поддръжка чрез DLP plug-in
- Осигуряване пълна видимост и контрол чрез изцяло интегрирана и централизирана конзола
- Намалява хардуерните изисквания посредством единен агент за антивирусна защита, управление на устройствата и управление на съдържанието посредством DLP

Интегрирано DLP решение за мрежови шлюзове

- Инспектира трафика в мрежата в реално време.
- Проследява и документира чувствителните данни, преминаващи през изходните мрежови точки.
- Идентифицира рисковани бизнес процеси и осигурява корпоративни полити за използване на данни.
- Реагира при неподходяща употеба на данни чрез ключови думи, регулярни изрази, бланки.
- Осигурява съответствие с нормативни уредби чрез употреба на външни шаблони.
- Speeds audits and enforcement with forensic data capture and real-time reporting Streamlines Administration, Lowers Costs
- Лесно внедряване и поддръжка чрез DLP plug-in
- Осигурява пълна видимост и контрол с изцяло интегрирано и централизирано решение
- Предоставя възможоност за автоматизирана реакция при нарушаване на политиките с опция за регистриране, заобикаляне, блокиране, криптиране, сигнализиране, карантина или изтриване на данни.

Централизирано решение за управление и наблюдение посредством Control Manager

Trend Micro Control Manager™ provides a convenient centralized security management console that consolidates policy, events and reporting across multiple iDLP solutions. This powerful security management tool lowers costs by simplifying security management, providing enterprise-wide visibility into managed products down to the individual client level. Control Manager also includes access to threat statistics from the Trend Micro Smart Protection Network™ cloud-based security infrastructure. Administrators gain insight into both the global threat landscape and the protective power of Trend Micro security in their own environment.

Protect Data at Rest, in Use, and in Motion

Data at rest with wide coverage of file types Trend Micro Integrated DLP can recognize and process over three hundred file types including most email and office productivity applications, programming languages, graphics, engineering files, and compressed or archived files. Discovery capabilities scan the mail store or SharePoint repository to see where compliance data is located. Data in motion control points Integrated DLP gives you visibility and control of data in motion—whether it's in email, webmail, instant messaging, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP. Data in use control points Integrated DLP provides visibility and control of data that's being used in USB ports, CDs, DVDs, COM & LPT ports, removable disks, floppy, infrared and imaging devices, PCMCIA, and modems. It can also be configured to monitor copy and paste and print screens.

Опростяване на DLP посредством темплетизирани политики

To help you quickly deploy data protection, Trend Micro Integrated DLP ships with wide range out-of-the-box templates, including (but not limited to): PCI/DSS — International standard for data security for credit cards. Any

company accepting credit cards are bound by these rules. HIPAA — The Health Insurance Portability and Accountability Act sets standards for any healthcare organization in the US. GLBA — Gramm Leach Bliley Act — Also known as the Financial Services Modernization Act, sets privacy regulations for banking, insurance, and investment companies. SB-1386 — Refers to state data breach laws. This particular law conforms to the California law which is the standard for most other U.S. states. US PII — Refers to personally identifiable information for US. This is a general catch-all for U.S. organizations concerned with protecting customer and employee data.

Data Identifiers

In addition to templates, Trend Micro Integrated DLP includes a granular list of truly international identifiers to identify specific data by patterns, formulas, positioning, and more. Identifiers can also be created from scratch.

7. ***Trend Micro Endpoint Application Control:***

Решението е интегрирано с останалите продукти на Trend Micro, целта му е да осигури защита на крайните точки срещу злонамерени софтуерни приложения, неоторизиран достъп и потребителски грешки.

- Предпазва машините и потребителите, които опитват да работят със злонамерени приложения.
- Получава всекидневно актуална информация за съществуващите заплахи.
- Предлага опция за създаване на "бели" и "черни" списъци на приложения по определени критерии, както и блокиране на непознати или нежелани приложения.
- Съществува опция за "блокиране на системата" да изпълнява нови приложения занапред.
- Осигурява разширени функции за прилагане на корпоративни политики и достигане на съответствие с регулаторни рамки.
- Осигурява съответствие с вътрешните ИТ технологии.
- Удобно централизирано управление и проследимост на потребителите чрез Trend Micro Control Manager.

8. ***Trend Micro Endpoint Encryption (Full Disk and File&Folder)***

Извършва цялостно крипиране на работните станции, преносими устройства, защита на отделни папки и файлове, позволява управление на ключовете посредством политики.

9. ***Vulnerability Protection (Virtual Patching)***

Защитава операционната система и приложенията от уязвимости и непознати заплахи.

10. ***PortalProtect Sharepoint Security***

Осигурява цялостна защита на SharePoint средата срещу вируси, шпионски софтуер, уеб заплахи, загуба на данни и други рискове, като прилага методи като уеб репутация, сканиране и филтриране на съдържанието, DLP решение.

11. *Cloud App Security*

Осигурява защита на облачната инфраструктура (Office 365, Google Apps, Box, Dropbox) срещу зловреден код,неоторизиран достъп, шпионски софтуер и други вируси.

12. *IM Security for Microsoft Lync and Office Communications Server*

Предоставя цялостна защита на комуникацията и съобщенията в реално време.

- Блокира зловредни линкове още преди да бъдат доставени.
- Открива и блокира непознати атаки, уеб заплахи, вируси, червеи, троянски коне, фишинг и друго неподходящо съдържание.
- Блокира шпионски софтуер, още преди да е достигнал работната станция.
- Филтрира съдържание и защитава от загуба на данни.
- Позволява лесно администриране чрез интегрирана платформа за работа и централизиран контрол.

IT CONSULTING COMPANY

София 1233
Бул. Сливница 141-143, етаж. 2
тел. +359 (2) 980 91 79

www.chorus.bg

ДО: **Софийска вода АД**

ПРИЛОЖЕНИЕ 4 –
„СПИСЪК НА ЛИЦАТА“

към **ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ** по обява **47410/ZB-3406**
за обществена поръчка на стойност по чл. 20, ал. 3 от ЗОП

В изпълнение на проекта по внедряване и поддръжка на Trend Micro Smart Protection Complete за нуждите на Софийска вода АД, Корус ООД ще ангажира следните служители:

1.

- Образование: **средно специално „компютърни системи“**
- Професионален опит с Trend Micro: **15 години**
- Сертификати:
  i. Trend Micro Certified Professional for Office Scan (от 2016 - приложен)
  ii. Trend Micro Certified Professional for Office Scan (от 2014 – приложен)

2.

- Образование: **висше – магистър „Комуникационна техника и технологии“**
- Професионален опит с Trend Micro: **15 години**
- Сертификати:
  i. Trend Micro Certified Professional for Office Scan (от 2016 - приложен)
  ii. Trend Micro Certified Professional for Office Scan (от 2014 – приложен)

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

TREND MICRO™ Certified Professional

USER PROTECTION

This certifies that

Has successfully completed the requirements to achieve the designation

Trend Micro Certified Professional for OfficeScan

On

15 September 2016

Eva Chen, Chief Executive Officer

TREND MICRO

Certified Professional

This certifies that

Has successfully completed the requirements to achieve the designation

Trend Micro Certified Professional for OfficeScan

On

31 March 2016

Eva Chen, Chief Executive Officer

TREND MICRO™ Education

This is to confirm that the candidate

—

Has successfully completed the requirements to achieve the title

Trend Micro Certified Professional for Deep Security

on 20 March 2014

Chief Executive Officer

TREND MICRO Education

This is to confirm that the candidate

Has successfully completed the requirements to achieve the title

Trend Micro Certified Professional for Deep Security

on 7 March 2014

Eva Chen
Chief Executive Officer

ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

Долуподписаният/ата/ **Владимир Младенов Александров**

/собствено бащино фамилно име /

в качеството си на **управител.**
/посочва се качеството на лицето/

в **КОРУС ООД**
/наименование на участника/

Относно: **„Надграждане на съществуващото решение на фирма Trend Micro за антивирусна защита на работните станции и сървъри на „Софийска вода" АД"**.

УВАЖАЕМИ ДАМИ И ГОСПОДА,

След запознаване с всички документи и образци от документацията за участие в процедурата за възлагане на обществена поръчка, потвърждаваме, че в случай, че бъдем избрани за изпълнител, ще изпълним поръчката, съобразно заложените в проекта на договор и неговите раздели - срокове, технически спецификации и изисквания на възложителя.

Известна ми е отговорността по чл.313 от Наказателния кодекс за посочване на неверни данни.

Документът се подписва от законния представител на участника или от надлежно упълномощено лице.

Дата: 28.01.2019 ..... Подпис и печат: .....

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

Образец

ДЕКЛАРАЦИЯ ЗА ПРИЕМАНЕ НА УСЛОВИЯТА В ПРОЕКТА НА ДОГОВОР

Обществена поръчка, възлагана чрез обява с предмет **„Надграждане на съществуващото решение на фирма Trend Micro за антивирусна защита на работните станции и сървъри на „Софийска вода" АД"**

С подаването на настоящия документ декларираме, че приемаме условията и ще подпишем, в случай че бъдем избрани Проекто-договора, включващи разделите и приложенията му, с които сме се запознали в качеството ни на участник в поръчката, възлагана чрез обява, и приложенията към нея.

С настоящото предлагаме да извършим дейностите предмет на обявата, на цени, които ще бъдат посочени в офертата ни, в съответствие на условията на проекта на договора включително разделите и приложенията.

Тази оферта остава валидна за срок от 6 месеца.

Минимален срок 5 месеца, считано от датата определена за краен срок за получаване на оферти.

Име: **Владимир Младенов Александров**

в качеството на: **управител**

Фирма/участник: **Корус ООД**

Адрес за кореспонденция: **София, бул. Сливница 141-143, ет. 2**

Телефон: 02/9809179 Факс: .....

Електронен адрес: **chorus@chorus.bg**

ЕИК/Булстат: **131152628**

Седалище и адрес на управление: **София, ул. Стара планина 15**

BIC:

IBAN:

Обслужваща банка:

Подпис: ..... Дата: 28.01.2019

Образец

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

Образец

Д Е К Л А Р А Ц И Я

Долуподписаният **Владимир Младенов Александров**, в качеството си на **управител** на фирма **КОРУС ООД**, при изпълнение на обществена поръчка възлагана чрез обява с предмет **„Надграждане на съществуващото решение на фирма Trend Micro за антивирусна защита на работните станции и сървъри на „Софийска вода" АД".**

Д Е К Л А Р И Р А М:

Намерение да използвам подизпълнител/и **.....НЕ.....**
(посочва се ДА или НЕ)

Забележка: Моля попълнете информацията по-долу, в случай че ще използвате подизпълнител/и.

Предвиждам да използвам в горепосочената процедура следните подизпълнители (посочва се: наименование на подизпълнителя, ЕИК/ЕГН):

.....
.....
.....
.....

Видове работи от предмета на процедурата, които ще се предложат на подизпълнители и съответстващият на тези работи дял в проценти от стойността на обществената поръчка:

.....
.....
.....

Дата: 28.01.2019 **Декларатор:** .....

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

VERACOMP EOOD
31 Cherni vrah, fl. 1, office 192
1421 Sofia, Bulgaria
mob. (+359) 898 750382
e-mail: office@veracomp.bg

София, 05.10.2018 г.

До: СОФИЙСКА ВОДА АД

Относно: Trend Micro партньорски статус на фирма Корус ООД

ОТОРИЗАЦИОННО ПИСМО

Уважаеми Дами и Господа,

С настоящото писмо, Веракомп ЕООД, със седалище в гр. София, Бул. Черни връх 31, офис 192, в ролята си на официален дистрибутор за Trend Micro на територията на Република България потвърждава, че фирма Корус ООД е оторизиран партньор за решенията на Trend Micro със златен статус на партньорско ниво според класификацията на производителя.

За контакт с производителя, можете да се свържете с г-н Жига Бенедик – Регионален Директор Trend Micro за България

С уважение:

/ – Директор Бизнес Развитие Trend Micro/

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

Заличена информация на основание ЗЗЛД и регламент ЕС2016/679.

TRANSPACIFIC CERTIFICATIONS LIMITED

BULGARIAN COPY
AMENDED DUE TO CHANGE IN SCOPE

Certificate of Registration
Сертификат за регистрация

This is to certify that
Настоящото удостоверява, че
Quality Management System of
Системата за Управление на Качеството на

КОРУС ООД
ул. „Стара планина" № 15,
гр. София 1000, България.

Complies with the requirements of
е в съответствие с изискванията на

ISO 9001:2015

This certificate is valid concerning all activities related to:
Сертификатът е валиден за всички дейности, свързани с:

ИТ консултантски услуги, предоставяне на облачни услуги, продажба на софтуер и хардуер, поддръжка на ИТ системи.

ANZSIC Code: 4222, 7000

12813 Certificate No. Сертификат No.	**Dec. 21, 2018** Date of this Certificate Дата на издаване	**Dec. 17, 2019** *Next Audit Due Date *Дата на следващ одит
Dec. 18, 2013 Date of Initial Registration Дата на първоначална регистрация	**Dec. 17, 2019** Certification Expiry Date Валидност на сертификата	Managing Director/Director Административен Директор/Директо

TRANSPACIFIC CERTIFICATIONS LIMITED

Website : www.tclcertifications.com E-mail : info@tclcertifications.com
Accreditation by Joint Accreditation System of Australia and New Zealand (Accreditation No. S2640303IN)
4 Phipps Close, DEAKIN, ACT 2600, AUSTRALIA
www.jas-anz.com.au/register