

DOKUMEN TENDER / RENCANA KERJA DAN SYARAT (RKS)

**Pengadaan Subscription Email Security
Tahun 2022**



JASA RAHARJA

A member of **IFG**

**Tim Pengadaan Subscription Email Security Tahun 2022
TAHUN 2022**

BAB I SYARAT UMUM & ADMINISTRASI

Dokumen Tender ini terdiri dari bagian yang tersebut dibawah ini dan berlaku sebagai acuan dalam mengajukan penawaran Tender Pengadaan Subscription Email Security Tahun 2022.

PASAL 1 KETENTUAN DAN ISTILAH

1. Dokumen Tender terdiri dari :
 - a. Syarat-syarat umum & administrasi (BAB I)
 - b. Ruang Lingkup Pekerjaan dan Spesifikasi Teknis (BAB II)
 - c. Metode Evaluasi (BAB III)
 - d. Berita Acara Pemberian Penjelasan dan lampirannya

2. Dokumen kontrak penyedia barang atau jasa terdiri dari :
 - a. Surat Perjanjian Pelaksanaan Pekerjaan/kontrak kerja
 - b. Dokumen Tender beserta berita acara penjelasan dan lampirannya.
 - c. Surat penawaran dan lampiran-lampirannya.
 - d. Pakta Integritas

Semua merupakan kesatuan yang tidak dapat dipisah-pisahkan.

3. Tim Pengadaan dan penyedia barang/jasa;
 - a. Tim Pengadaan adalah sekumpulan orang yang ditugaskan untuk melaksanakan Tender Pengadaan Pengadaan Subscription Email Security Tahun 2022.
 - b. Penyedia barang/jasa adalah pihak yang akan diserahkan tugas melaksanakan pengadaan seperti yang akan dijelaskan lebih lanjut dalam RKS ini.

PASAL 2 PEMBERIAN PENJELASAN

1. Rapat pemberian penjelasan diadakan secara virtual pada :
Hari : akan diberitahukan melalui undangan
Tanggal : sda
Jam : sda

2. Pada saat pemberian penjelasan harus dihadiri secara virtual oleh Direktur penyedia barang/jasa, dalam hal tidak hadir dapat diwakilkan kepada pejabat yang berwenang dengan membawa **surat tugas** yang ditandatangani diatas kertas berkop perusahaan dan dicap serta bermeterai secukupnya dan dilampiri foto copy KTP masing-masing / tanda pengenal.

PASAL 3 TENDER

1. Tender pekerjaan Pengadaan Pengadaan Subscription Email Security Tahun 2022, diselenggarakan berdasarkan Keputusan Direksi PT Jasa Raharja nomor KEP/90.3/2020 tanggal 30 April 2020 tentang Standar Prosedur Operasi Pengadaan Barang dan Jasa.
2. Peserta Tender adalah penyedia barang/jasa yang merupakan badan usaha yang memiliki persyaratan sebagai berikut ;
 - a. Terdaftar sebagai rekanan pada aplikasi *e-procurement* PT. Jasa Raharja;
 - b. Memiliki Akte pendirian perusahaan dan perubahan terakhir (jika ada);
 - c. Memiliki NPWP dan Surat Pengukuhan Pengusaha Kena Pajak (PKP);
 - d. Memiliki TDP atau NIB yang masih berlaku;
 - e. Memiliki SIUP yang masih berlaku
 - f. Memiliki SITU / Keterangan Domisili Perusahaan yang masih berlaku;
3. Peserta Tender yang mengajukan penawaran harus telah;
 - a. Mendaftar pengadaan melalui aplikasi E-Procurement PT. Jasa Raharja melalui website eprocurement.jasaraharja.co.id;
 - b. Diundang oleh Tim Pengadaan Pengadaan Subscription Email Security Tahun 2022;
 - c. Mempelajari dan memahami semua dokumen Tender;
 - d. Mengikuti rapat pemberian penjelasan (aanwijzing);
 - e. Mengetahui semua prosedur Tender;
4. Pemasukan penawaran akan diadakan pada :
Hari : akan disepakati pada saat pemberian penjelasan (aanwijzing)
Tanggal : sda
Dimulai jam : sda
Ditutup jam : sda
Tempat di : sda

Sesaat setelah ditutupnya pemasukan surat penawaran, apabila jumlah penawaran yang masuk ternyata **kurang dari 3 (tiga)**, maka sesuai Keputusan Direksi PT Jasa Raharja Nomor KEP/90.3/2020 tanggal 30 April 2020 tentang Standar Prosedur Operasi Barang dan Jasa, tetap dilanjutkan pembukaan surat penawaran dengan peserta yang ada.

5. Penawaran yang datang setelah penutupan akan ditolak dan dinyatakan gugur.

PASAL 4 SURAT PENAWARAN DAN LAMPIRAN-LAMPIRAN

1. Pemasukan dan pembukaan dokumen penawaran ditetapkan dengan Sistem 1 (satu) sampul. penyampaian dokumen penawaran dengan sistem ini bahwa dokumen penawaran yang berisi persyaratan administrasi dan teknis dimasukkan ke dalam sampul tertutup pertama, sedangkan, dokumen penawaran yang berisi harga penawaran dimasukkan ke dalam sampul tertutup kedua, selanjutnya sampul pertama dan sampul kedua dimasukkan ke dalam sampul penutup dan disampaikan kepada Tim Pengadaan atau petugas yang ditunjuk.

2. Keseluruhan dokumen penawaran dimasukkan kedalam satu sampul/amplop, yang mencakup semua persyaratan dan dokumen sesuai dengan permintaan yang ditentukan di dalam dokumen pengadaan.
3. Dokumen penawaran mencakup surat penawaran yang dilengkapi persyaratan administrasi, teknis, dan perhitungan harga yang ditanda-tangani oleh penyedia barang/jasa sebagaimana dipersyaratkan di dalam dokumen pengadaan;
4. Pada sampul luar ditulis nama paket pekerjaan, nama dan alamat peserta, serta ditujukan kepada **Tim Pengadaan** Subscription Email Security Tahun 2022 dengan alamat yang ditentukan dalam dokumen pengadaan;
5. Harga penawaran dalam dokumen penawaran dicantumkan dengan jelas. Detail untuk harga penawaran.;
6. Dokumen penawaran bersifat rahasia sampai batas waktu pemasukan penawaran berakhir;
7. Penawaran yang diterima diluar jadwal waktu yang telah ditetapkan dalam dokumen pengadaan dinyatakan gugur.
8. Surat penawaran dan lampiran-lampirannya diserahkan kepada Tim Pengadaan sebelum penutupan pemasukan penawaran.
9. **Pemasukan dan pembukaan dokumen penawaran harus dihadiri oleh masing-masing Direktur Penyedia Barang/Jasa, dalam hal tidak hadir dapat diwakilkan kepada pejabat yang berwenang dengan membawa surat kuasa yang ditandatangani diatas kertas berkop perusahaan, dicap perusahaan dan bermeterai secukupnya dan dilampiri foto copy KTP masing-masing.**
10. Penyedia barang / jasa diwajibkan mengajukan Surat Penawaran dan formatnya tidak ditentukan secara khusus, minimal menyangkut :
 - a. Nama dan alamat Direktur atau Pimpinan Perusahaan;
 - b. Nilai harga penawaran beserta rincian biaya;
 - c. Jangka waktu pelaksanaan;
 - d. Perincian spesifikasi / ruang lingkup pekerjaan yang ditawarkan;
 - e. Harga yang tercantum dalam surat penawaran bersifat lumpsum fixed price, termasuk pajak-pajak yang menjadi kewajiban.
11. **Penyedia barang atau jasa diwajibkan upload dokumen penawaran berupa Surat Penawaran Harga dan kelengkapannya yang telah di scan dengan bentuk file PDF ke e-procurement Jasa Raharja sesuai dengan waktu yang telah ditentukan oleh Tim Pengadaan.**
11. Surat penawaran harus dibuat diatas kertas berkop nama perusahaan serta harus ditanda tangani oleh Direktur atau Pimpinan Perusahaan atau Pejabat yang berwenang dalam perusahaan tersebut dan dicap perusahaan dengan menyebutkan nama jelas.
12. Surat penawaran dibuat rangkap 2 (dua) lengkap dengan lampiran-lampirannya dan surat penawaran yang asli bermeterai dan cap perusahaan. Surat penawaran termasuk lampiran lampirannya dijilid menjadi satu buku kemudian dimasukkan kedalam sampul surat penawaran yang tertutup.

(Nama PT)

Dokumen Penawaran
Pengadaan Subscription Email Security Tahun 2022

Kepada :
Tim Pengadaan Subscription Email Security Tahun 2022



13. Urutan penjilidan buku dokumen penawaran sbb;

Tahap 1	Tahap 2 (Jika Lolos Tahap 1)
a. Data Administrasi	a. Data Penawaran
a. Copy Akte pendirian perusahaan dan perubahan terakhir (jika ada). b. Copy NPWP dan Copy Surat Pengukuhan Pengusaha Kena Pajak (PKP) c. Copy TDP atau NIB yang masih berlaku d. Copy SIUP yang masih berlaku e. Copy SITU/Keterangan Domisili Perusahaan yang masih berlaku f. Laporan keuangan Tahun Buku 2021 (diutamakan yang telah diaudit) g. Surat Dukungan Principle h. Dokumen Kualifikasi i. Copy Jaminan Penawaran dan surat pernyataan bahwa Jaminan Penawaran tersebut adalah benar, asli dan sah yang ditandatangani oleh pihak penerbit Surat Jaminan Penawaran di atas meterai cukup (asli diserahkan kepada panitia)	1. Surat Penawaran Harga 2. Lampiran rincian harga

b. Data Teknis
a. Spesifikasi Teknis b. Daftar Pengalaman Pekerjaan dalam pengadaan sejenis (melampirkan copy kontrak) c. Jangka Waktu Pelaksanaan

14. Bagi penyedia barang/jasa yang mengundurkan diri setelah penunjukan pemenang, maka jaminan penawaran akan dicairkan dan menjadi milik PT Jasa Raharja.

15. Dalam Tender ini akan dilakukan evaluasi secara sistem Merit Poin.

16. Surat penawaran harga dan biaya kirim harus bersifat lumpsum fixed price dan termasuk pajak pajak yang menjadi kewajibannya.

17. Surat penawaran harus diserahkan kepada tim pengadaan sampai batas waktu yang telah ditentukan setelah mengisi daftar hadir.

18. Jaminan penawaran ditetapkan senilai 1% s.d 3% dari jumlah harga penawaran **yang diterbitkan oleh bank pemerintah/swasta atau perusahaan asuransi yang mempunyai program Surety Bond** dan akan diberikan tanda terima oleh Tim Pengadaan dengan syarat sbb:
 - a. Jaminan penawaran ditujukan kepada **Tim Pengadaan Subscription Email Security Tahun 2022**, Jl. H.R. Rasuna Said Kav.C-2 Jakarta Selatan 12920, masa berlaku jaminan penawaran minimal selama 90 (sembilan puluh) hari kalender.
 - b. Jaminan penawaran tersebut akan dikembalikan setelah penyedia barang/jasa menyerahkan jaminan pelaksanaan dan kontrak ditandatangani.
 - c. Bagi penyedia barang/jasa yang menang dalam Tender ini, selanjutnya membuat jaminan pelaksanaan sebesar 5 %.

19. Surat penawaran dianggap tidak sah/gugur apabila;
 - a. Penawaran yang disampaikan oleh penyedia barang/jasa yang tidak diundang dalam Tender ini.
 - b. Tidak ditandatangani oleh peserta atau tidak distempel perusahaan yang bersangkutan (dalam hal kekurangan ini, dapat dipenuhi pada saat pembukaan Tender). Namun apabila pada saat itu tidak dapat dipenuhi, maka penawaran ybs. dinyatakan gugur.
 - c. Tidak jelas besarnya jumlah penawaran dengan angka dan dengan huruf.
 - d. Tidak mencantumkan jumlah penawaran dengan angka maupun dengan huruf.
 - e. Tidak melakukan upload dokumen penawaran harga dalam *e-procurement*.
 - f. Melakukan upload dokumen penawaran harga dalam *e-procurement* tetapi tidak hadir dalam pemasukan dan pembukaan penawaran.

21. Apabila harga penawaran yang tercantum dalam angka tidak sesuai dengan yang terbilang dalam huruf maka penawaran yang dipakai adalah nilai yang sesuai dengan dokumen pendukung.

PASAL 5 PEMBUKAAN PENAWARAN

1. Pembukaan penawaran dilakukan tim pengadaan pada waktu yang telah ditentukan.
2. Sebagai unsur pemeriksaan semua wakil Tender mendampingi tim pengadaan dalam pemeriksaan surat penawaran yang masuk. Keputusan sah atau tidaknya suatu penawaran berada ditangan tim pengadaan.
3. Atas pembukaan sampul dan penetapan sah atau tidaknya surat penawaran, harga-harga penawaran dan lain-lain peristiwa pada penyelenggaraan Tender dibuat berita acara pembukaan surat penawaran yang ditandatangani oleh tim pengadaan dan seluruh wakil peserta.
4. Dalam hal pembukaan Penawaran, Tim Pengadaan dilakukan secara online melalui Aplikasi E-Procurement, maka Berita Acara Pembukaan dicetak melalui system E-Procurement dan dianggap sah.

5. Berdasarkan evaluasi penawaran, Tim Pengadaan segera menetapkan nominasi calon pemenang dari peserta yang memasukkan penawaran yang paling menguntungkan, dalam arti penawaran secara teknis yang baik dengan harga yang dapat dipertanggung jawabkan.
6. Dalam hal terdapat dua atau lebih penawaran dengan harga terendah sama dan secara teknis baik serta memiliki kecakapan dan kemampuan relatif sama, maka Tim Pengadaan meminta kepada peserta tersebut untuk mengajukan penawaran harga baru dan dituangkan dalam Berita Acara.

PASAL 6 HAK SANGGAH

Untuk menjamin adanya transparansi dan perlakuan yang sama dalam Pengadaan Subscription Email Security Tahun 2022, maka pihak yang kalah berhak mengajukan sanggahan, dengan ketentuan :

1. Sanggahan hanya berkaitan dengan kesesuaian pelaksanaan Tender dengan prosedur atau tata cara Tender yang tercantum dalam dokumen Tender.
2. Sanggahan hanya dilayani apabila pihak penyanggah telah menyetorkan uang jaminan sanggahan sebesar nilai jaminan penawaran dan disertai bukti-bukti yang kuat kepada tim pengadaan.
3. Sanggahan harus diajukan dalam waktu selambat-lambatnya 2 (dua) hari kalender mulai sejak diumumkan pemenang.
4. Tim pengadaan akan menyampaikan keputusan atas sanggahan tersebut selambat-lambatnya 14 (empat belas) hari kalender dari tanggal diterimanya pengajuan sanggahan.
5. Uang jaminan sanggahan tersebut dikembalikan kepada penyanggah apabila sanggahannya terbukti benar secara hukum dan menjadi hak Jasa Raharja apabila sanggahannya tidak terbukti secara hukum.

PASAL 7 PENARIKAN DIRI

1. Penarikan diri sebagai peserta hanya dapat dilakukan sebelum acara pembukaan surat penawaran dimulai.
- 2. Penarikan diri setelah pembukaan surat penawaran mengakibatkan jaminan penawaran yang telah diserahkan menjadi milik PT Jasa Raharja.**
3. Dalam hal pemenang pertama mengundurkan diri, maka pemenang urutan kedua ditunjuk untuk melaksanakan pengadaan, demikian seterusnya kepada pemenang ketiga.
4. Apabila pemenang yang ditunjuk tidak bersedia melaksanakan pekerjaan, maka jaminan penawaran para pemenang yang ditunjuk menjadi milik PT Jasa Raharja.

PASAL 8 TENDER ULANG

Tender atas Pengadaan Subscription Email Security Tahun 2022 ini dinyatakan diulang, apabila terdapat kondisi sebagai berikut :

1. Jumlah calon peserta Tender yang memenuhi persyaratan untuk diundang kurang dari 3 (tiga) peserta.
2. **Tidak ada peserta** yang menyampaikan dokumen penawaran.
3. Jika hasil evaluasi Tim Pengadaan menunjukkan bahwa tidak ada penawaran yang memenuhi persyaratan administrasi dan teknis sebagaimana yang ditentukan di dalam dokumen pengadaan.
4. Tidak ada penawaran yang harga penawarannya dibawah atau sama dengan dana (nilai pagu) yang tersedia.
5. Terdapat sanggahan dari peserta Tender yang ternyata dapat dibuktikan kebenarannya
6. Dalam evaluasi penawaran ditemukan indikasi atau bukti terjadinya persaingan tidak sehat.
7. Pemenang pertama, kedua dan ketiga tidak bersedia ditunjuk sebagai pelaksana pekerjaan.
8. Dalam pelaksanaan Tender terdapat indikasi atau bukti terjadinya pelanggaran atas prinsip dasar, etika dan/atau norma pengadaan barang/jasa,

PASAL 9 PEMUTUSAN HUBUNGAN KERJA

1. Tanpa mengurangi hak-hak yang dimiliki oleh PT Jasa Raharja, apabila penyedia barang/jasa lalai dan tidak bertindak menurut ketentuan yang tercantum dalam Surat Perjanjian Pelaksanaan Pekerjaan atau perintah dari PT Jasa Raharja, maka PT Jasa Raharja dapat memutuskan hubungan kerja dalam hal ini:
 - a. Tanpa alasan yang dapat diterima menanggukkan atau menunda sama sekali pelaksanaan pengadaan sebelum selesai;
 - b. Penyedia barang/jasa tidak dapat melanjutkan pengadaan dengan kesungguhan;
 - c. Penyedia barang/jasa menolak atau dengan tegas mengabaikan peringatan tertulis dari PT Jasa Raharja.
2. Tanpa mengurangi hak-hak yang dimiliki oleh PT Jasa Raharja, apabila penyedia barang/Jasa setelah 3 (tiga) kali berturut-turut tidak mengindahkan peringatan peringatan tersebut atau dalam pelaksanaan selanjutnya melakukan kelalaian yang sama, maka PT Jasa Raharja tanpa mengurangi hak-hak lainnya dalam waktu

7 (tujuh) hari sejak pengulangan atau penerusan kelalaian dapat segera memutuskan surat Perjanjian Pelaksanaan Pekerjaan dengan penyedia barang/jasa secara tertulis.

PASAL 10 TEMPAT PERADILAN

1. Bilamana terjadi perselisihan mengenai hal-hal yang menyangkut pelaksanaan pengadaan, maka hal ini akan diselesaikan dengan cara musyawarah,
2. Bilamana dengan cara musyawarah belum juga diperoleh kata sepakat, Maka kedua belah pihak sepakat untuk memilih domisili Pengadilan yang tetap dan tidak berubah pada Pengadilan Negeri Jakarta Selatan.

PASAL 11 RISIKO UPAH DAN HARGA

Dalam pelaksanaan pengadaan ini fluktuasi upah, harga atau komponen lainnya yang terjadi selama masa pelaksanaan Pengadaan Subscription Email Security Tahun 2022 ini menjadi risiko penyedia barang / jasa.

PASAL 12 PERATURAN PEMBAYARAN

Peraturan pembayaran untuk Pengadaan Subscription Email Security Tahun 2022 menggunakan sistem kontrak secara Lumpsum dan akan diatur kemudian sesuai dengan kesepakatan yang akan dituangkan dalam Surat Perjanjian Pelaksanaan Pekerjaan.

PASAL 13 JAMINAN PELAKSANAAN

Pelaksana pekerjaan wajib menyerahkan Jaminan Pelaksanaan sebesar 5 % (lima perseratus) dari nilai pekerjaan **yang diterbitkan oleh bank pemerintah/swasta atau perusahaan asuransi yang mempunyai program Surety Bond** untuk jangka waktu sesuai dengan kemampuan penyedia barang / jasa dimana jangka waktu pelaksanaan minimal 60 (enam puluh) sejak kontrak ditandatangani.

PASAL 14 JANGKA WAKTU PENYELESAIAN PEKERJAAN

Jangka waktu maksimal yang diberikan kepada penyedia barang/jasa untuk menyelesaikan seluruh Pengadaan Subscription Email Security Tahun 2022 dalam RKS ini adalah **30 (tiga puluh) hari kalender**. Jangka waktu sebagaimana dimaksud di atas agar dicantumkan di dalam Surat Penawaran.

BAB II RUANG LINGKUP PEKERJAAN DAN SPESIFIKASI TEKNIS

1. RUANG LINGKUP DAN SPESIFIKASI

No.	Nama Perangkat	Deskripsi	Jumlah
	Proofpoint P0 Bundle - SaaS		
1	PP-B-POF-S-B-104	PFPT Enterprise P0 - F-Secure- S. NPRE, Email Protection, TAP URL & Attachment Defense, TAP URL Iso. (VAP only), Threat Response Auto-Pull - F-Secure - SaaS, 1001 users. Included : PP-SUP-PS12, Platinum Level Support, 1001 users (12 Months)	1
2	PP-PST-IS-IMP	InfoSec PS Implementation Services	1
	Local Services		
1	MT-JKT06-PS-Proofpoint	Installation fee (JKT)	1
2	MT-SWM-8-854-Proofpoint	MTID 8x5 Local Maintenance for 1 year with 8 visit max per year (4-Corrective & 4-Preventive visit for Jakarta Area)	1

1. Pengadaan Subscription License Email Security Proofpoint P0 Bundle-SaaS dengan spesifikasi :
 - a. Memiliki license sebanyak 1001 user
 - b. Memiliki masa subscription selama 1 tahun
 - c. Solusi berupa layanan cloud
 - d. Berupa layanan bundle yang terdiri dari Email Protection Server (PPS), Targeted Attack Protection (TAP), Threat Response Auto-Pull (TRAP), URL Isolation for VAPs.
 - e. Termasuk Platinum Level Support
2. Instalasi dan Konfigurasi
 - a. Melakukan site survey, diskusi, dan memberikan rancangan terhadap *topology* dan *logical design* dari sistem disesuaikan secara *best practice* dengan perangkat yang ditawarkan.
 - b. Menyediakan jasa instalasi, konfigurasi, update dan testing untuk semua perangkat yang ditawarkan termasuk komponen pendukungnya sesuai dengan solusi/layanan yang ditawarkan
 - c. Melakukan instalasi dan initial setup cloud email security beserta aktivasi lisensi
 - d. Melakukan switch over traffic mail dari sistem existing ke sistem cloud
 - e. Melakukan konfigurasi Targeted Attack Protection (TAP)
 - f. Melakukan konfigurasi URL Rewriting dan Attachment Sandboxing
 - g. Melakukan konfigurasi Threat Response Auto-Pull (TRAP)
 - h. Melakukan konfigurasi anti spoofing (contoh: SPF, DMARC, DKIM)
 - i. Mengintegrasikan solusi cloud email security dengan sistem Microsoft Exchange, Microsoft Exchange Online/O365, Microsoft Active Directory
 - j. Monitoring dan Fine Tuning
 - k. User Acceptance Test
3. Maintenance & Support yang mencakup dukungan layanan gangguan 24x7 melalui telepon, email, chat kepada technical support.

- a. On Site Support apabila permasalahan tidak dapat diselesaikan melalui Off Site Support (8x5).
- b. Preventive Maintenance 4x /tahun
- c. Response Time : 30 menit
- d. Software and Patch Update
- e. Support Area : Jakarta

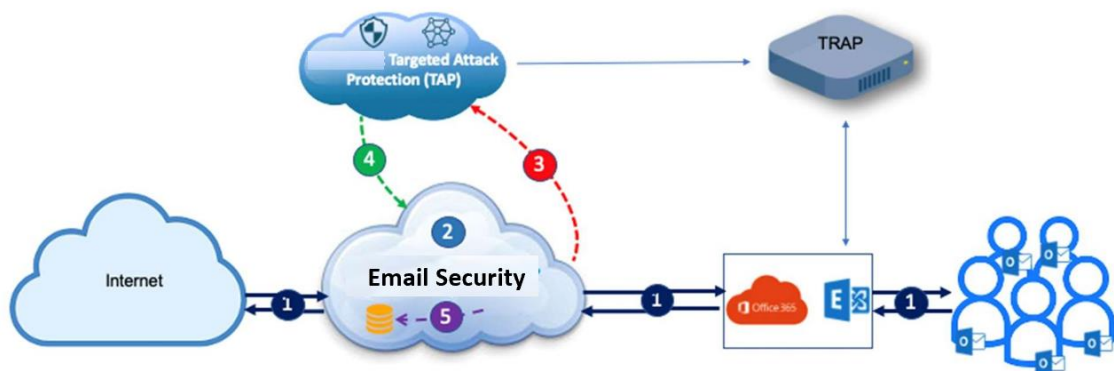
a. Tenaga Ahli

Pelaksana pekerjaan Subscription Email Security memerlukan tenaga ahli yang berkualifikasi sebagai berikut :

- Jumlah Tenaga Ahli minimal 2 orang.
- Berpendidikan minimal S1
- Berpengalaman minimal 1 tahun di bidang system yang ditawarkan
- Memiliki sertifikasi PACSE (Proofpoint Accredited Channel Sales Engineer) minimal 1 orang.

2. Spesifikasi Teknis

a. Network Topology



b. Spesifikasi Detail

a) General

1. Solusi harus menyediakan perlindungan terhadap serangan dan gangguan email seperti email impostor, phishing, malware, spam, bulk(gray), adult dan low priority email.
2. Solusi harus menggunakan deployment on cloud
3. Solusi harus memiliki kemampuan untuk di perbesar skala nya tanpa menimbulkan masalah.
4. Solusi harus menyediakan fitur message tracing tingkat lanjut.
5. Solusi harus menyediakan laporan real time untuk visibilitas yang detail tentang mail flow dan trend.
6. Layanan dari solusi dapat diberikan white-label untuk memberikan keakraban bagi end user.
7. Solusi harus mendukung beragam bahasa.

8. Solusi harus mendukung minimum 2 mail transfer agents (MTA) untuk email masuk dan keluar sehingga solusi dapat menerima dan memproses koneksi concurrent email yang besar.
9. Solusi harus mendukung integrasi dengan data external seperti LDAP.
10. Solusi harus recursively unpack compressed dan zipped files.
11. Solusi harus menyediakan fitur connection Throttling.
12. Solusi harus support SNMP v3.
13. Solusi harus tersinkronisasi dengan waktu enterprise menggunakan protokol NTP atau Secure NTP.
14. Solusi harus dapat memberikan capability untuk mitigate perubahan denial of service (DoS) attack.
15. Solusi harus menyediakan mekanisme perlindungan dari serangan directory harvest

b) Spam/Malware

1. Solusi harus menyediakan perlindungan terhadap inbound dan outbound email spam
2. Solusi harus menyediakan customer untuk memilih salah satu email engine dari beberapa anti virus.
3. Solusi harus mendukung deteksi Business Email Compromise dan email impostor melalui teknologi machine learning daripada statik ruleset.
4. Solusi harus memiliki kemampuan menangkap email dengan kategori "Adult"
5. Solusi harus menyediakan pengklasifikasi spam seperti adult, bulk mail, impostor, malware, phish, suspected spam untuk membuat policy lebih granular
6. Solusi yang diusulkan harus memberikan Circle of Trust email classifier untuk protects pada small group users dimana ada high-value targets atau executives pada Organization dari unwanted email dan unfamiliar senders.
7. Solusi yang diusulkan harus dapat meng-identifikasi inappropriate dan registered images.
8. Solusi yang diusulkan harus dapat melakukan deteksi malformed SMTP packets.
9. Solusi harus mendukung deteksi multi language spam.
10. Solusi harus menyediakan kemampuan pengaturan level spam.
11. Solusi harus menyediakan kemampuan untuk silently drop SMTP connections pada connection level berdasarkan reputation.
12. Solusi harus menyediakan kemampuan untuk mendeteksi new spam campaigns hampir secara real-time.
13. Solusi yang diusulkan harus melindungi organization dari ancaman advanced email threats – termasuk zero-day threats, ransomware, polymorphic malware, weaponized documents, dan credential phishing attacks.
14. Solusi yang diusulkan harus dapat segera quarantine messages dengan malicious URLs, dan rewrite semua URLs untuk track dan block clicks.

15. Solusi yang diusulkan harus dapat melakukan analisa waktu click untuk mencegah access ke site jika URL menjadi buruk.
16. Solusi yang diusulkan harus dapat menggunakan combination secara static dan dynamic technology untuk menerapkan multi-stage analysis inspect untuk memeriksa attack chain.
17. Solusi yang diusulkan harus dapat memberikan predictive analysis untuk pre-emptively identify dan sandbox suspicious URLs berdasarkan email traffic patterns.
18. Solusi yang diusulkan harus menangkap threats yang tidak meninggalkan digital yang jelas, seperti credential phishing attacks.
19. Solusi yang diusulkan harus dapat memiliki ability untuk mencegah malware untuk menghindari detection dengan recognizing evasive attacker techniques
20. Solusi yang di gunakan harus menggabungkan dan memanfaatkan platform dari community-based intelligence yang mencakup email, network, mobile apps, dan social media vectors, serta verified threat intelligence diluar dari domains and IP addresses.
21. Solusi yang diusulkan harus menghasilkan alerts on any message yagn mungkin delivered, tetapi di kembalikan sebagai malicious.
22. Solusi yang diusulkan harus memiliki kemampuan manually move all instances dari malicious emails user inbox termasuk cc, bcc dan forwarded mails kedalam quarantine mailbox untuk mencegah users untuk membuka atau clicking.
23. Solusi yang diusulkan harus memastikan bahwa setiap safe-listed domains atau email addresses tidak dikirim malicious content ke end users atau bypass modul spam detection.
24. Solusi yang diusulkan harus secara dynamically ditambahkan tag ke inbound messages untuk di peringatkan atau inform users bahwa untuk incoming message yang mungkin dangerous. Tags ditambahkan pada incoming message berdasarkan results dari content scan engines.

c) **Phishing / Spoofing / BEC**

1. Solusi harus mampu mendeteksi Business Email Compromise (BEC) dan email impostor emails memalui machine learning daripada ruleset yang statik
2. Solusinya harus mendeteksi serangan lower-volume targeted phishing.
3. Solusi harus mendukung pembuatan rule custom phishing .
4. Solusi harus membuat repository dari display name untuk user email dalam organisasi yang sering ditarget oleh serangan email impostor. Mampu membatasi email address yang legitimate untuk masuk ke inbox organisasi
5. Solusi harus mendukung fitur dimana administrator bisa melakukan export dan import Impostor Display Names List dalam format CSV.

d) **Detection/Protection Capabilities**

1. Solusi harus menggunakan kombinasi teknik static dan dynamic detection
2. Solusi yang diusulkan harus dapat menyertakan targeted attack attribution yang di targetkan untuk peningkatan pemahaman konstektual tentang attack.

e) **URLs**

1. Solusi yang diusulkan harus menggunakan big-data analysis dan machine-learning heuristics untuk identify malicious URLs yang akurat.
2. Solusi yang diusulkan harus bisa melihat versi "normalized" dari URL di scoring engine.
3. Solusi yang diusulkan harus dapat menyediakan pre-emptive sandboxing sebelum user kesempatan untuk melakukan click.
4. Solusi yang diusulkan harus dapat re-write URLs untuk track dan block clicks pada click time.
5. Solusi yang diusulkan harus dapat rewrite scheme-less URLs didalam emails.
6. Solusi yang diusulkan harus dapat memberikan granularity untuk memilih apakah re-write URLs dalam bentuk text or HTML message bodies.
7. Solusi yang diusulkan harus dapat secara automatically move all instances emails dengan malicious URLs yang dikirim ke all users inbox termasuk cc, bcc dan forwarded instances didalam quarantine mailbox mencegah users clicking berdasarkan URL sandboxing verdict.
8. Solusi yang diusulkan harus dapat membuat unique policies untuk URL rewrite policies groups users atau members Sub-Org yang berbeda.
9. Solusi yang diusulkan harus dapat menunjukkan original destination visible ke user dengan hovering over rewritten URL pada saat message displays yang original
10. Solusi yang diusulkan harus dapat memberikan opsi untuk seamlessly integrate dengan URL browser isolation platform ketika user clicks link rewritten pada email body, maka akan diarahkan ke isolation environment dimana user bebas untuk scroll halaman tetapi tidak dapat upload or download dan melakukan tekan tombol apapun sampai tidak ada yang berbahaya akan di kembalikan dari platform, user kemudian akan diberikan allowed untuk keluar dari isolation environment.
11. Solusi yang diusulkan harus dapat memberikan Plain Text untuk URL rewrite untuk menambahkan domain ke URL label.

f) **Attachments**

1. Solusi yang diusulkan harus dapat mengamati commonly exploited file attachments seperti MS office dan PDF documents untuk identify suspicious yang menunjukkan adanya indicates advanced malware.
2. Solusi yang diusulkan harus dapat melakukan validasi attachments melalui hash valuedari attachments tersebut.
3. Solusi yang diusulkan harus dapat use hash value attachments sebagai filter value untuk search logs.
4. Solusi yang diusulkan harus memiliki automatically move all instances mails dengan malicious attachments yang dikirimkan ke all users inbox termasuk cc, bcc and forward yang diteruskan ke quarantine mailbox untuk mencegah users dari clicking berdasarkan attachment sandboxing verdict.

g) **Email Policy**

1. Solusi harus memiliki kemampuan untuk pemfilteran dan perutean email berbasis expression yang fleksibel, berbasis policy, dan menggunakan header dan menilai dari isi email.
2. Solusi harus memiliki kemampuan untuk mengubah nilai header SMTP, seperti menambah / menghapus x- headers, modifikasi baris subjek, penulisan ulang alamat, dll.
3. Solusi harus menawarkan banyak pengaturan seperti pengupasan lampiran, pengiriman pemberitahuan ke pengirim, dan karantina seluruh email.
4. Solusi harus menerapkan aturan khusus pada email yang berisi perlindungan kata sandi atau file terenkripsi.
5. Solusi harus memiliki kemampuan untuk menambahkan keyword ke baris subjek berdasarkan rule policy.
6. Solusi harus menetapkan aturan berbeda berdasarkan alamat email tertentu.
7. Solusi harus memiliki kemampuan untuk mengaktifkan penandaan BATV(Bounce Address Tag Validation) berdasarkan domain atau policy, termasuk kapan harus menerapkan penandaan BATV dalam perutean email.

h) **Email Authentication**

1. Solusi harus mendukung kebijakan granular untuk Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), dan Domain Message Authentication Reporting & Conformance (DMARC).
2. Solusi harus memiliki kemampuan untuk melakukan verifikasi penerima terhadap Active Directory dan sumber daftar email lainnya.
3. Solusi harus mendukung validasi Authentication Received Chain (ARC) untuk kumpulan domain tepercaya untuk kasus penggunaan pengirim pihak ketiga di mana autentikasi DMARC mungkin gagal

i) **Quarantine**

1. Solusi harus memiliki kemampuan karantina email.
2. Solusi harus mengatur email ke dalam folder karantina yang ditentukan.
3. Solusi harus mengizinkan administrator untuk melihat, merutekan ulang, atau melepaskan email di karantina.
4. Solusi harus mengizinkan user menerima email yang dikarantina dan mengakses karantina user untuk merilis email. Semua rilis surat harus dicatat.
5. Solusi harus menyediakan folder karantina terpisah untuk email Phishing tanpa mengizinkan akses apa pun oleh user.
6. Solusi tersebut harus memiliki kemampuan bagi administrator untuk melihat pratinjau email yang dikarantina untuk menentukan tindakan lebih lanjut yang harus diambil.

j) **Email Routing**

1. Solusi harus memiliki kemampuan untuk merutekan email atau salinan email secara selektif ke tujuan internal atau eksternal lainnya, termasuk opsi untuk mengirim email

sebagai lampiran, opsi untuk menandai email dengan konten khusus atau filter / status atau skor kebijakan, dll.

2. Solusi tersebut harus mendukung Izinkan Relay dari Alamat IP Office 365 dan dapat memilih paket dari daftar rentang alamat IP berdasarkan langganan paket layanan Microsoft tanpa impor manual.

k) End-user Experience, Appearance & Management

1. Solusi harus mendukung penyisipan satu atau beberapa rule policy di email keluar atau masuk.
2. Solusi harus diterapkan secara selektif berdasarkan aturan policy atau tidak berlaku jika email dienkripsi s / mime atau ditandatangani secara digital, dll.
3. Solusi harus mendukung multi-bahasa di signature/disclaimers.
4. Solusi harus menerapkan signature and disclaimers berdasarkan grup pengguna AD.
5. Solusi harus memiliki kemampuan untuk memasukkan konten dinamis di signature/disclaimers seperti tanggal dan waktu, dll.
6. Solusi harus dapat menginformasikan spam digest dan durasi email digest harus dapat dikonfigurasi.
7. Solusi harus memungkinkan user untuk merilis email, mengelola daftar white list dan blacklist mereka sendiri dan melaporkan false negatif dan false positif langsung dari email intisari spam.
8. Solusi harus mendukung semua pelaporan email false negatif dan false positif.
9. Solusi harus mendukung otentikasi dua faktor untuk user dan administrator.
10. Solusi harus mengubah warna layar login, header untuk antarmuka manajemen, dan judul untuk web-UI
11. Solusi harus mengizinkan administrator untuk mengubah batas maksimum jumlah email yang akan disertakan dalam email digest

l) Management

1. Solusi harus menyertakan manajemen berbasis web dan konsol konfigurasi tanpa memerlukan plug-in atau add-on.
2. Solusi harus mendukung administrasi berbasis delegasi.
3. Solusi harus mendukung otentikasi lagi penyimpanan data pengguna lokal, LDAP atau sumber Active Directory, atau melalui penyedia identitas organisasi itu sendiri (melalui SAML).
4. Solusi harus menyediakan administrator fasilitas untuk manajemen antrian email.
5. Solusi harus memungkinkan administrasi yang didelegasikan ke dalam sub-organisasi.
6. Solusi harus memiliki kemampuan untuk menetapkan thresholds untuk menginformasikan tim IT Security.

7. Solusi harus membatasi ukuran email yang dapat dikirim / diterima dan / atau jumlah penerima dalam sebuah email.
8. Solusi harus membatasi pemeriksaan SMTP dan memeriksa validitas informasi amplop sebelum menerima email untuk pengiriman.
9. Solusi yang diusulkan harus dapat memberikan informasi spesifik tentang pengguna mana yang telah menerima dan / atau mengklik URL di email yang mencurigakan.
10. Solusi yang diusulkan harus membatasi login dari alamat IP tertentu atau blok CIDR alamat.

m) **Search**

1. Solusi harus termasuk memiliki kemampuan message-tracing untuk membantu pekerjaan helpdesk.

n) **Reporting**

1. Solusi harus mempunyai kemampuan reporting yang bersifat summary dan detail termasuk penjadwalan untuk dikirim melalui email
2. Solusi harus memiliki kemampuan mencari sembarang email yang melewati system dalam waktu 15 menit.
3. Solusi harus menyediakan kebijakan untuk mengaudit pesan masuk dan keluar.
4. Solusi harus menyediakan audit trail yang mendekati real time.
5. Solusi harus menyediakan pelaporan berhubungan dengan spam dan malware.
6. Solusi yang diusulkan harus dapat menyediakan dashboard grafis berbasis web yang menyediakan data di tingkat organisasi, ancaman, dan pengguna serta memberikan dukungan informasi forensik untuk investigasi insiden keamanan serangan email.
7. Solusi yang diusulkan harus dapat menyediakan intelijen kampanye malware dan laporan forensik.
8. Solusi yang diusulkan harus dapat memberikan pelaporan terperinci untuk waktu click events URL.
9. Solusi yang diusulkan harus menyediakan kemampuan untuk menyimpan salinan lokal dari peristiwa keamanan dan metadata dari email yang dipertukarkan untuk kegiatan forensik.
10. Solusi yang diusulkan harus menyediakan kemampuan untuk memantau daftar pengguna VIP dalam organisasi terhadap kemungkinan serangan spoofing nama tampilan.
11. Solusi yang diusulkan harus dapat memberikan kemampuan untuk memantau indeks serangan personel yang menjadi sasaran dan juga menelusuri apa saja ancaman yang menargetkan mereka.
12. Solusi yang diusulkan harus mampu memberikan kemampuan untuk membuat daftar orang-orang yang paling diserang dalam suatu organisasi untuk memungkinkan tim keamanan memfokuskan upaya pada orang-orang yang menjadi sasaran.

BAB III METODE EVALUASI TENDER

SISTEM EVALUASI

Metode evaluasi Tender Pengadaan Subscription Email Security Tahun 2022 menggunakan Sistem Nilai (merit point). Sistem nilai merupakan evaluasi penilaian penawaran dengan cara memberikan nilai angka tertentu pada setiap unsur yang dinilai, berdasarkan kriteria dan bobot yang telah ditetapkan dalam dokumen pengadaan, kemudian membandingkan jumlah nilai dari setiap penawaran peserta dengan penawaran peserta lainnya.

Evaluasi Tender menggunakan Sistem Merit Point dimana untuk evaluasi administrasi menggunakan Sistem Gugur dan untuk evaluasi teknis Sistem Merit Point. Sistem merit point digunakan untuk menganalisa dan mengevaluasi aspek teknis dari solusi yang ditawarkan yang diwujudkan dalam bentuk pembobotan point untuk masing-masing aspek teknis tersebut. Dalam hal ini bobot 55% (lima puluh lima perseratus) diberikan terhadap kesesuaian spesifikasi teknis pengadaan dan 45% (empat puluh lima perseratus) diberikan terhadap evaluasi harga.

Urutan proses penilaian dengan sistem merit point adalah sebagai berikut :

a. Evaluasi Administrasi:

- 1). Evaluasi administrasi dilakukan terhadap penawaran yang memenuhi syarat pada pembukaan penawaran;
- 2). Evaluasi administrasi dilakukan terhadap dokumen penawaran yang masuk dan dievaluasi kelengkapan dan keabsahan syarat administrasi. Unsur-unsur yang dievaluasi pada tahap ini harus berdasarkan ketentuan yang tercantum di dalam dokumen pengadaan.

Setiap rekanan wajib menyampaikan persyaratan administrasi minimal terdiri dari :

- a. Copy Akte pendirian perusahaan dan perubahan terakhir (jika ada).
- b. Copy NPWP dan Copy Surat Pengukuhan Pengusaha Kena Pajak (PKP)
- c. Copy TDP atau NIB yang masih berlaku
- d. Copy SIUP I yang masih berlaku
- e. Copy SITU/Keterangan Domisili Perusahaan yang masih berlaku
- f. Laporan keuangan Tahun Buku 2021 (diutamakan yang telah diaudit)
- g. Surat Dukungan Principle
- h. Dokumen Kualifikasi;
- i. Copy Jaminan Penawaran dan surat pernyataan bahwa Jaminan Penawaran tersebut adalah benar, asli dan sah yang ditandatangani oleh pihak penerbit Surat Jaminan Penawaran di atas meterai cukup (**asli diserahkan kepada panitia**)

Seluruh persyaratan tersebut diatas, **wajib** dipenuhi oleh peserta Tender/ penyedia barang sebagai persyaratan untuk dapat diikuti sertakan pada tahapan evaluasi selanjutnya. Pada saat evaluasi administrasi, setiap rekanan wajib menunjukkan asli dokumen jika diminta. Apabila penyedia barang tidak dapat melengkapi seluruh persyaratan administrasi tersebut diatas, maka penawaran

dari penyedia barang / jasa tersebut tidak diikutsertakan dalam evaluasi selanjutnya dan dinyatakan kalah.

- 3). Evaluasi administrasi menghasilkan dua kesimpulan, yaitu memenuhi syarat atau tidak memenuhi syarat administrasi dan jika evaluasi administrasi menyatakan tidak lulus, maka penawaran dianggap gugur dan jika evaluasi administrasi menyatakan lulus, maka akan dilanjutkan dengan evaluasi teknis.

b. Evaluasi Teknis (Bobot 55%):

- 1). Evaluasi teknis dilakukan terhadap penawaran yang dinyatakan memenuhi persyaratan atau lulus administrasi;
- 2). Adapun unsur yang dinilai pada evaluasi teknis adalah sebagai berikut :
 - a. Kesesuaian spesifikasi teknis (sub bobot 40%).
 - b. CV dan Sertifikat Tenaga Ahli (sub bobot 20%)
 - c. Pengalaman dalam pengadaan serupa lebih dari 2 tahun (sub bobot 15%).
 - d. Jangka waktu pelaksanaan pengadaan (sub bobot 25%).
- 3). Dari total 55% bobot yang ada, berikut pembobotan detail dari aspek teknis yang dipersyaratkan :

1.	Kesesuaian Spesifikasi Teknis (40%)	Nilai
	a. Spesifikasi Teknis sesuai b. Spesifikasi Teknis tidak sesuai	100 0
	CV dan Sertifikat Tenaga Ahli (20%)	100
	a. Melampirkan CV dan Ijazah b. Tidak Melampirkan	0
2.	Pengalaman dalam pengadaan sejenis (15%)	Nilai
	a. ≥ 2 tahun atau nominal kontrak \geq Rp. 1 Miliar	100
	b. < 2 tahun nominal kontrak $<$ Rp. 1 Miliar	50
	c. Tidak memiliki pengalaman	0
3.	Jangka Waktu Pelaksanaan (25%)	Nilai
	a. Sesuai RKS	100
	b. Tidak sesuai RKS	0

Batas minimal nilai kelulusan untuk evaluasi teknis adalah 70

c. Evaluasi Harga (Bobot 45%) :

Meliputi evaluasi kewajaran harga dan kerendahan harga :

- 1) Evaluasi Kewajaran Harga (Sub bobot 50%)
Evaluasi kewajaran harga penawaran dilakukan dengan membandingkan harga yang ditawarkan oleh peserta pengadaan dibandingkan dengan Harga Perkiraan Sendiri (HPS) yang telah ditetapkan, namun tidak lebih tinggi dari HPS dan juga tidak lebih rendah 20% (dua puluh perseratus) dari HPS.

- 2) Evaluasi Kerendahan Harga (Sub bobot 50%)
Evaluasi kerendahan harga penawaran dilakukan dengan membandingkan antara harga penawaran yang bersangkutan dengan harga yang terendah. Harga terendah yang memenuhi syarat adalah maksimal 20% (dua puluh perseratus) dari HPS.

Demikian Dokumen Tender ini dibuat sebagai acuan dalam mengajukan penawaran Tender Pengadaan Subscription Email Security Tahun 2022.

Jakarta, 11 Juli 2022

Tim Pengadaan Subscription Email
Security Tahun 2022.



 Margareth Panjaitan
Ketua Tim